IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE

PLAINTIFF'S RESPONSE AND COUNTER-STATEMENT TO DEFENDANTS' STATEMENT OF UNDISPUTED MATERIAL FACTS

Pursuant to Rule 56 of the Federal Rules of Civil Procedure and Rule 56.1 of the Local Rules of the United States District Court for the Southern District of New York, Plaintiff U.S. Securities and Exchange Commission (the "SEC") respectfully submits this Response and Counter-Statement to Defendants SolarWinds Corp. and Timothy G. Brown's Statement of Undisputed Material Facts ("Def. 56.1")[1] (ECF No. 182), submitted in support of their motion for summary judgment.

To the extent that the SEC does not dispute a particular assertion by Defendants, the SEC does not thereby concede that any such undisputed assertion constitutes a material fact, or that the cited evidence is relevant, or that it would be admissible at trial. Nor does the SEC thereby

[1] Citations to "JS __" refer to the parties' Joint Statement of Undisputed Facts (ECF No. 166). Citations to "Def. Ex. __" refer to the exhibits attached to the concurrently filed Declaration of Serrin Turner in Support of Defendants' Motion for Summary Judgment. Citations to "[Last Name] Decl." refer to the concurrently filed declarations of Rani Johnson, Steven Colquitt, Danielle Campbell, Robert Krajcir, Lee Zimmerman, Tim Brown, and Gregory Rattray. Citations to "SEC Ex. __" refer to the exhibits attached to the Declaration of Kristen Warden in Support of Plaintiff SEC's Opposition to Defendants' Motion for Summary Judgment filed concurrently with this Response and Counter-Statement to Defendants' Statement of Undisputed Material Facts.

admit the truth of those assertions for purposes other than the resolution of Defendants' motion. To the extent that the SEC does not dispute assertions that a witness testified to a particular fact or that a document contains a specific statement, the SEC does not thereby concede that the witness or document is credible or admissible on that point, that the substance of the testimony or statement is not disputed, or that the testimony or statement is accurate or relevant. The SEC does not hereby respond to the assertions of fact made in the subheadings.[2]

I. DOCUMENT THE SEC RELIES ON AS TO THE NIST CYBERSECURITY FRAMEWORK REPRESENTATION

1. The only document the SEC cites as relevant to the NIST Cybersecurity Framework is a draft of a "policy documentation audit" emailed to Tim Brown on April 19, 2021 (after the Relevant Period), from which the SEC cites language stating that "about 40% of the baseline controls within NIST [800-53] were met or partially met."[3]

SEC Response: Disputed. Although the SEC does not dispute that Ms. Pierce sent the referenced e-mail to Mr. Brown on April 19, 2021, the SEC disputes Defendants' contention that this document is the "only document the SEC cites as relevant to the NIST Cybersecurity Framework" as misleading and limited solely to documents listed in the Joint Statement of Undisputed Facts. In addition to the email from Ms. Pierce, the SEC also refers to the following documents, among other things, as relevant to the NIST Cybersecurity Framework: (i) an October 1, 2018 e-mail from Mr. Quitugua to individuals, including Mr. Brown, attaching an excel file mapping critical security controls to the NIST Cybersecurity Framework [SEC Ex. 4 [SW-SEC00013676-3677]; *see also* Am. Compl. ¶83 and SEC 56.1 ¶¶241-243; and (ii) various

[2] For the convenience of the Court, footnotes 3 through 191 herein are copied from and maintain the same numbering as in Def. 56.1.

[3] JS ¶157; Def. Ex. 41 (SW-SEC00185450) at -451.

documents containing "scorecards" for reflecting NIST maturity levels, [*see* SEC Ex 2 [Brown Dep.] 187:10-15 ("[T]he NIST scorecard is part of this entire process....we put together this program around the NIST CSF and the assessments that we did in each one of these areas.")], including August 16, 2019 and November 15, 2019 "Security & Compliance Program Quarterly" presentations [SEC Ex. 5 [SW-SEC00001497-1550] (cited in SEC 56.1 ¶¶244-250); Def. Ex. 28 [SW-SEC00001551]], and "Quarterly Risk Review" presentations from March 2020 [Def. Ex. 37 [SW-SEC00001608]; Def. Ex. 38 [SW-SEC00001602]], and October 2020 [Def. Ex. 40 [SW-SEC00001582]].

The SEC further disputes Defendants' characterization of the document in paragraph 1 as a "policy documentation audit," as the document's full title is "Solar Winds Executive Policy *and Procedures* Documentation Audit – Executive Summary DRAFT." [Def. Ex. 41 [SW-SEC0018540] (emphasis added)].

2. This referenced audit reviewed the extent to which the Company had *policy documentation* in place corresponding to the controls in NIST Special Publication 800-53 ("NIST 800-53"). It was not an audit of whether the Company had implemented NIST 800-53 controls in practice.[4]

SEC Response: Disputed. Defendants' description of the document in paragraph 1 is incomplete and misleading. In fact, the document does refer to the extent to which NIST 800-53 controls were, or were not, implemented. For example, under the "Summary Conclusion" heading, Ms. Pierce writes: "As of the date of testing, SolarWinds is still in the process of

[4] Def. Ex. 41 (SW-SEC00185450) at -451 (referencing the document as a "policy and procedures documentation audit"); *id.* (explaining that objective was to prepare policies for "annual policy reviews" and that scope of review only encompassed "policy documentation").

updating the policies and procedures *and designing and implementing many of the NIST 800-53 recommended controls*." [Def. Ex. 41 [SW-SEC00185450], at -5451 (emphasis added)].

3. This was specifically labeled a draft document and was based only on policy documentation currently in SolarWinds' policy library and policy guidance already published by Human Resources and Legal.[5]

SEC Response: Undisputed.

4. After receiving this draft, Tim Brown asked the person who prepared it how the results would change if it included policies that were currently being drafted or under review. The drafter responded that "we could probably get up to 80% compliance."[6]

SEC Response: Undisputed that the quoted statements were made, but the SEC disputes that "we could probably get up to around 80% compliance" is an undisputed fact as it is speculation and therefore cannot be presented in the form of admissible evidence.

5. In any event, NIST 800-53 is distinct from the NIST Cybersecurity Framework ("NIST CSF") referenced in the Security Statement.[7]

SEC Response: Disputed. The term "distinct" is vague and ambiguous in this context. The SEC does not dispute that the NIST Cybersecurity Framework does not automatically incorporate NIST 800-53. But, as Mr. Graff stated, while "there is not a requirement that they adhere to any particular [set of controls]" [Def. Ex. 50 [Graff Dep.] 106:25-107:1], there are "menus" of controls that an entity can select, including 800-53 [*id*. at 106:9-12; *see also* JS ¶¶62-63]. Ms. Johnson further testified that SolarWinds' security controls were based on NIST 800-

[5] Def. Ex. 41 (SW-SEC00185450) at -451.

[6] Def. Ex. 42 (SW-SEC-SDNY_00046821) at -821.

[7] JS ¶63; Def. Ex. 50 (Graff Dep.) 106:21-107:8 (the NIST cybersecurity "framework does not set up any kind of requirement for them to adhere to all of the controls in 8[00-]53.").

53. [SEC Ex. 52 [Johnson Dep.] 159:21-160:1 ("The security controls leveraged [800-53] for the basis of identifying areas of focus and to standardize on a common language and framework to talk about security.")].

6. NIST 800-53 is a standard, which requires an organization to have specific controls in place in order to meet it. The NIST CSF is not; it is a voluntary self-evaluation framework.[8]

SEC Response: Undisputed.

7. Following the NIST CSF does not imply that an organization meets any specific controls—including NIST 800-53 controls.[9]

SEC Response: Undisputed, except to the extent Defendants imply that "following"' NIST means that SolarWinds had robust cybersecurity controls and/or adhered to cybersecurity best practices, which is a factual question for the jury.

8. While an organization may choose to use NIST 800-53 "as an informative reference" in evaluating itself under the NIST CSF, doing so is voluntary and does not turn the NIST 800-53 into "a checklist that must be completed" by the organization.[10]

SEC Response: Disputed. Though the SEC does not dispute that "While an organization may choose to use NIST 800-53 'as an informative reference' in evaluating itself under the NIST CSF, doing so is voluntary," the SEC disputes the phrase "does not turn the NIST 800-53 into 'a checklist that must be completed' by the organization" as an improper legal conclusion. The extent to which an organization may need to comply with NIST 800-53, or disclose its failures to

[8] JS ¶¶ 47, 62-63.

[9] JS ¶62; Def. Ex. 50 (Graff Dep.) 106:21-107:8 (agreeing that "following the NIST cybersecurity framework [doesn't] infer from that that they meet any specific control").

[10] JS ¶63; Def. Ex. 45 (Bliss Dep.) 84:12-15 (explaining that NIST CSF is a "voluntary framework").

comply with NIST 800-53 (or portions thereof) in order to make statements the organization has made about its compliance with the NIST Cybersecurity Framework not misleading is a mixed question of fact and law that requires factual determinations. If an organization states it "follows" the NIST Cybersecurity Framework, chooses to use NIST 800-53 to evaluate itself regarding the NIST Cybersecurity Framework, and determines that it has utterly failed numerous criteria in 800-53, then its statement regarding following the NIST Cybersecurity Framework may be misleading by omission.

9. Accordingly, whether SolarWinds followed the NIST CSF is not determined by the extent to which SolarWinds had NIST 800-53 controls in place (whether in documentation or in practice).[11]

SEC Response: Disputed. See response to paragraph 8.

II. DOCUMENTS THE SEC RELIES ON AS TO THE ROLE-BASED ACCESS CONTROLS REPRESENTATION

A. June 2017 Slide Proposing More Granular Controls for Administrators' Accounts

10. The SEC cites a slide from a deck titled "Securing Active Directory," drafted by Brad Cline (SolarWinds' Director of IT) and dated June 2017, well before the publication of the Security Statement and the Relevant Period. The SEC cites a slide from the deck titled "Current assessment," which refers in part to "an unnecessary level of risk within our environment," stating "[s]ystem team currently runs as Domain Admin."[12]

SEC Response: Undisputed.

---

[11] Def. Ex. 2 (Rattray Rep.) ¶¶ 30-39, 111; Def. Ex. 45 (Bliss Dep.) 125:14-22 (describing NIST 800-53 as "a set of specific controls that … are for heightened standards …").

[12] JS ¶158; Def. Ex. 6 (SW-SEC00262012) at -013.

11. The slide does not concern any pervasive failure to implement the principle of least-privilege access or role-based access controls.[13]

SEC Response: Disputed. Defendants' use of the phrase "does not concern any pervasive failure" in paragraph 11 is conclusory and unsupported by the cited materials. Mr. Cline stated in testimony, "There were newer tech that was coming out that could allow the ability for us to apply a *more granular privilege model to their role*, but we needed to review it." [Def. Ex. 49 [Cline Dep.] 107:8-11 (emphasis added)]. Despite Mr. Cline's testimony, the document cited in paragraph 11 on its face states under "[p]ath forward": "[i]mplement a least-privileged based administrative model" and "[i]mplement managed service accounts and remove any elevated service accounts." [Def. Ex. 6 [SW-SEC00262012], at -2014]. A reasonable juror could conclude from the plain language of Mr. Cline's testimony and this document that a plan to implement these items meant that SolarWinds did not have least privileged access or managed service accounts in place as of June 2017, the date of the document cited in paragraphs 10 and 11.

12. The slide specifically related to a small team of system administrators managed by Mr. Cline.[14]

---

[13] Def. Ex. 49 (Cline Dep.) 106:12-111:22 ("[T]here were a few different folks on that team, they would have had a least-privilege model around their access levels."), 95:17-22 (noting that assessment related to "15 accounts running as domain admin.").

[14] Def. Ex. 49 (Cline Dep.) 95:17-22 (noting that assessment related to "15 accounts running as domain admin."), 102:19-103:18 (discussing the "context" of this slide deck was that Cline "had just taken on the system administration team" and that this was referring to "the system administrators within that group."), 106:2-24 ("[T]his is very specific to that team, the systems administration team[.]"), 107:1-16 (noting he was assessing access "for a select few system administrators."), 117:12-120:10 (noting he was "just look[ing] specifically at the domain admin group"), 125:10-128:6.

SEC Response: Disputed. On its face, the document cited in paragraphs 10 through 12 references accounts beyond just those held by systems administrators, including "5 Domain Admin level service accounts with passwords unchanged as far back as 2007." In response, the ensuing pages of the document state as a "[p]ath forward" to "[i]mplement a least-privilege based administrative model" such that "[n]o user or service account would use domain admin, any login attempt would trigger an alert." [Def. Ex. 6 [SW-SEC00262012], at -2013-14]. This language suggests an issue larger in scope than just Mr. Cline's staff and is an issue of fact for the jury.

13. The slide was not about the team members having administrative privileges they did not need for their role. The team members were system administrators who needed administrative privileges for the systems they managed.[15]

SEC Response: Disputed. This is a misleadingly incomplete description of the document. The slide at issue is titled "[c]urrent assessment" and identifies an "unnecessary level of risk within our environment," including that there are "15 accounts running as Domain Admin," "5 Domain Admin level services accounts with passwords unchanged as far back as 2007," and that the "[s]ystem team currently runs as Domain Admin [with a] high level of risk during routine operations." [Def. Ex. 6 [SW-SEC00262012], at -2013]. In his testimony, Mr. Cline stated that he was considering the potential application of "Just-in-Time privilege administration" such that "you will only receive access to your administrative role when you need it and then it goes away after you're done. With least privilege you would have only rights

[15] Def. Ex. 49 (Cline Dep.) 99:2-17 ("So the systems team in the course of their job needs domain admin to do their job[.]"), 106:12-24, 125:10-128:6 ("So this is referring to our system administrators. And removing admin rights for all roles – was not a possible technical thing for us to perform. They wouldn't be able to do their jobs without using admin rights."), 127:5–19 ("Their job was to be a domain administrator. … So the idea that we could remove their domain administrative accounts means they couldn't do their job.").

to the lowest model needed for your role, which depending on your role could be domain admin, but there are other roles that may not require domain admin that could be more granular within the systems administrator team." [Def. Ex. 49 [Cline Dep.] 102:19-103:10]. Given this context, a reasonable juror could understand that SolarWinds personnel at certain times held a greater level of administrative privileges than necessary to perform their role.

14. The slide was about ideas Mr. Cline had for a more granular layer of controls that would enable the team members to use their privileged accounts only during certain tasks requiring them and to switch to non-privileged accounts for more routine operations.[16]

SEC Response: Disputed for the reasons stated in response to paragraphs 12 and 13.

15. The ideas were based on "newer tech that was coming out" that provided for such granular controls.[17]

SEC Response: Undisputed.

16. In other words, the slide was about an opportunity, related to a small set of employees, to refine role-based access controls that already existed, rather than a finding that role-based access controls were lacking.[18]

SEC Response: Disputed. Paragraph 16 does not accurately characterize the cited document. On its face, the first substantive page of the document under "Current assessment" states that "We have an unnecessary level of risk" [Def. Ex. 6 [SW-SEC00262012], at -2013],

---

[16] Def. Ex. 49 (Cline Dep.) 96:19-97:9 ("[S]ome recent changes within Active Directory … gave you the ability to implement more granular controls around domain administration."), 102:19-103:10 (discussing how "some newer technologies" allowed you to "be more granular within the systems administration team."); 106:12-24, 107:7-108:10, 112:2-16.

[17] Def. Ex. 49 (Cline Dep.) 107:1-16 ("There were newer tech that was coming out that could allow the ability for us to apply a more granular privilege model").

[18] Def. Ex. 49 (Cline Dep.) 95:17-22 (noting that assessment related to "15 accounts running as domain admin."); 107:1-16.

and offers a "[p]ath forward" that SolarWinds "[i]mplement a least-privileged based administrative model," that "[n]o user or service account would use domain admin, any login attempt would trigger an alert" [*Id*. at -2014].

B. Documents about Efforts to Centralize and Automate Access Provisioning

1. January 2018 Slide about Evaluation of Access Management Tools

17. The SEC cites a slide deck dated January 2018 titled "User Access Management: Tool Evaluation & Recommendation," in particular to language referring to "a collection of people who have access to many systems and many people involved in provisioning access" and a statement that "[t]he lack of standardized user access management processes that captures user provisioning … across the organization create a loss risk of organizational assets and personal data."[19]

SEC Response: Undisputed. It is also undisputed that the slide deck further states that "it was discovered that there is no organization-wide, standardized approach to access management that includes provisioning, changing and de-provisioning users access to systems that contain personal information." [Def. Ex. 10 [SW-SEC00043618], at -3621].

18. The slide deck does not concern any pervasive failure to implement the principle of least-privilege access or role-based access controls.[20]

SEC Response: Disputed. The phrase "does not concern any pervasive failure" is conclusory and unsupported by the cited materials. The only fact witness support for this paragraph is the Johnson Declaration, which itself acknowledges that "with many help desk staff involved in provisioning user access…manual configuration of these systems created the

[19] JS ¶165; Def. Ex. 10 (SW-SEC00043618) at -621.

[20] Johnson Decl. ¶ 10; Def. Ex. 10 (SW-SEC00043618) at -621 (noting that there is no single "organization-wide standardized approach to access management," not a lack of process generally).

potential for error…" [Johnson Decl. ¶10]. Additionally, a reasonable juror could understand the contemporaneous statement that there was "a collection of people who have access to many systems" to reflect a pervasive failure to implement the principle of least-privileged access and choose to credit that contemporaneous plain language over the post-hoc rationale provided by Ms. Johnson.

19. The slide deck is about an evaluation of tools SolarWinds was considering using to automate the technical aspects of provisioning users with access rights.[21]

SEC Response: Disputed. The SEC does not dispute that the slide deck was in part about automating the technical aspects of provisioning users with access rights but disputes that this short summary fairly characterizes the entire contents of the document. Additionally, the SEC notes that the cited Brown deposition testimony does not refer to the January 2018 "User Access Management" slide deck [Def. Ex. 10 [SW-SEC00043618]], but rather the August 2019 "Security & Compliance Program Quarterly Overview" [SEC Ex. 5 [SW-SEC00001497-1550]] in connection with which Mr. Brown was testifying regarding the basis for a NIST Maturity Level 1 finding as to the "Security Category" of "Authentication, Authorization and Identity Management" [*id.* at -1507; *see also* SEC Ex. 2 [Brown Dep.] 183:8-20 (describing August 2019 Security & Compliance Program Quarterly Overview and marking it as Brown Exhibit 14), 183:20-221:25 (discussing document)]. The Brown testimony accordingly is not specifically referring to the meaning of Def. Ex. 10.

[21] Johnson Decl. ¶¶ 9-10; Def. Ex. 46 (Brown Dep.) 208:8-14 ("So we had … manual processes for on-boarding employees and giving them rights to certain, uh, certain systems or certain applications. And that process worked, uh, but we had not automated that process with a tool. We were going through and, uh, consolidating—we still had a Google directory service and a Azure directory service. We were consolidating to Azure.").

20. SolarWinds had a process in place at this time for provisioning users with access based on their role—the SARF process.[22]

SEC Response: Disputed. The SEC disputes paragraph 20 to the extent it attempts to modify the language, and therefore the meaning, of JS ¶74. That paragraph reads "SolarWinds had a process in place *designed* to provision users with access based on what they needed for their role" [JS ¶74 (emphasis added)] and does not mean that the procedures were performed perfectly or without fail [*see id.* at 12 n.2]. The other cited testimony similarly does not address the uniformity or successful implementation of the SARF process.

21. However, the SARF process was relatively manual, in that implementing a SARF often required IT personnel to separately configure access rights on a number of different systems to provision the employee with access to all the systems they needed.[23]

SEC Response: Undisputed.

22. The more systems that IT personnel needed to separately configure, the more chances there were for errors to be made in the provisioning and deprovisioning process.[24]

SEC Response: Undisputed.

23. This slide deck was about finding an identity access and management ("IAM") tool that would enable IT personnel to provision user access rights using one centralized system

---

[22] JS ¶ 74; Def. Ex. 45 (Bliss Dep.) 237:21-238:7 (describing SARF process generally); Def. Ex. 59 (Kim Dep.) 97:11-19 (noting SARF process was in place to address user access).

[23] Def. Ex. 46 (Brown Dep.) 204:15-22 (noting that SARF was a "manual process to onboard people"); Def. Ex. 45 (Bliss Dep.) 237:18-238:13 (same); Johnson Decl. ¶ 10.

[24] Johnson Decl. ¶¶ 7, 10; Def. Ex. 45 (Bliss Dep.) 238:17-24 ("SARF—a manual process … prone to isolated incidents such as a form not being filled out accurately or the access rights not being provisioned on a perfectly timely basis, but those were very isolated. The more you could automate that, the thought was you could reduce those isolated exceptions.").

and automatically configure access rights on the downstream systems, thereby minimizing the risk of errors.[25]

SEC Response: Disputed. The SEC does not dispute that the slide deck was in part about finding an IAM tool but disputes that this short summary fairly characterizes the entire contents of the document. On the face of the document, it also includes a "[p]roblem statement" reflecting its purpose in identifying a "lack of standardized user access management process that captures user provisioning" among other findings quoted in paragraph 17 and the SEC's response thereto. [Def. Ex. 10 [SW-SEC00043618], at -3621].

24. The Company chose to move forward with migrating to Microsoft Azure Active Directory ("Azure AD") as its IAM tool for this purpose.[26]

SEC Response: Undisputed.

25. The fact that the SARF process was a relatively manual process prior to this migration being completed did not contradict the Security Statement, which did not make any representations that the Company's access provisioning process was automated in any respect.[27]

---

[25] Johnson Decl. ¶¶ 8-13; *see also* Def. Ex. 49 (Cline Dep.) 69:6-19 ("We were always looking for ways to automate anything that was a manual task within IT … . In particular, SARF was one of the things that we had looked at as an area that we could do more automation in."); Def. Ex. 52 (Johnson Dep.) 103:14-21 ("Azure active directory … was a replacement for an older technology, active directory on prem that was highly federated. The point of the identity and access management project, which put Azure AD in the cloud, was a way to centralize identity across all of the three different business units.").

[26] Johnson Decl. ¶ 8; Def. Ex. 49 (Cline Dep.) 141:14-142:4; Def. Ex. 52 (Johnson Dep.) 102:22-103:8, 183:12-19; Def. Ex. 46 (Brown Dep.) 209:19-210:1; Def. Ex. 45 (Bliss Dep.) 234:3-19; Def. Ex. 47 (Brown Inv. Vol. I) 286:17-287:24 ("[T]he process was manual. The process went through and had—it essentially worked but it had humans involved, and whenever humans are involved, it's not as efficient and it's not as prescriptive as what we would like it to be. So this is calling out that one of the places where we need to improve is absolutely the identity management side of the world, making it more automated, making it more controlled.").

[27] Def. Ex. 1 (Security Statement) at 3; Def. Ex. 50 (Graff Dep.) 213:24-215:29-22 ("And I did double-check what you said about role-based access control. It doesn't say anything about it being automated.").

SEC Response: Disputed. Paragraph 25 is conclusory and its statement that the manual nature of the SARF process does not contradict the Security Statement is unsupported by the cited evidence. While the paragraph purports to be supported by a citation to the testimony of Mr. Graff (*i.e.*, "It doesn't say anything about it being automated." [Def. Ex. 50 [Graff Dep.] 213:24-215:22]), within that the same line of questioning, Mr. Graff in response to the question "[I]f what this was highlighting was that the access controls were limited in that sense, there was no contradiction with what the security statement says?" responded that "Yeah, I think that would be very speculative on my part to agree with that. I mean, it seems to me that the clear reading is that there was a problem they were trying to point out." [Def. Ex. 50 [Graff Dep.] 214:11-20].

26. The fact that SolarWinds was seeking to improve its access provisioning process does not imply that it pervasively failed to implement role-based access controls.[28]

SEC Response: Disputed. While, the SEC does not dispute that an attempt to improve a process does not automatically prove whether that process was or was not adequate before the attempt to improve it, the SEC does dispute the implication within the assertion in paragraph 26 that the document cited in paragraph 17 was only about an attempt to improve the access provisioning process, as any such implication is supported only by speculation and conjecture.

2. September 2018 Slide about Limited Access Management Tooling

27. The SEC also cites a September 2018 deck titled "Incident Review," which, in the appendix after the "Thank You" page, includes a slide from which the SEC quotes a line in red

[28] Def. Ex. 50 (Graff Dep.) 208:24-209:3 ("I could imagine that customers would want to move to an integrated single sign-on system for many reasons, not necessarily because their role-based control has failed.").

text stating "Identity Management – Role and Privilege Management," along with a legend indicating that red font means "Limited or non existent."[29]

SEC Response: Undisputed. It is also undisputed that the same slide deck identified nine incidents from January 1, 2018, to September 10, 2018, that "had/have the potential to cause serious damage" including "[e]levated RMM access credentials exposed in publicly available Google Doc and if exploited would allow access to all data in RMM" and "[t]est server with production data and on [sic] the open internet with no security and default password." [SEC Ex. 17 [SW-SEC00386134-43], at -6139].

28. This text was a reference to the limited IAM and Privileged Access Management ("PAM") *tooling* at the Company, which it was seeking to remedy through the planned migration to Azure AD as well as through the rollout of a PAM tool known as "Thycotic." It was not referring to any lack of role-based access controls at the Company.[30]

SEC Response: Disputed. Paragraph 28 is not supported by the cited evidence, and the emphasized term "tooling" is vague. Neither the Brown declaration nor his cited testimony refer to the September 2018 deck. The referenced paragraph from the Brown declaration reiterates and confirms a portion of the Johnson declaration ("As Ms. Johnson explains in her declaration, which I have reviewed..." and "I have reviewed Ms. Johnson's Declaration on this topic and agree with her statements.") [Brown Decl. ¶9 (citing Johnson Decl. ¶¶4-18)]. The Johnson declaration in turn does not mention this document. The cited Brown deposition testimony is referring to Brown Exhibit 14 (August 2019 "Security & Compliance Program Quarterly

[29] JS ¶171; Def. Ex. 16 (SW-SEC00386134) at -143.

[30] Brown Decl. ¶ 9; Def. Ex. 46 (Brown Dep.) 208:8-14 ("So we had again manual processes for on-boarding employees and giving them rights to certain [] systems or certain applications. And that process worked, [] but we had not automated that process with a tool. We were going through and, [] consolidating – we still had a Google directory service and a Azure directory service. We were consolidating to Azure.").

Overview") [SEC Ex. 5 [SW-SEC00001497-1550]], in connection with which Mr. Brown was testifying regarding the basis for a NIST Maturity Level 1 finding as to the "Security Category" of "Authentication, Authorization and Identity Management" [*id.* at -1507; *see also* SEC Ex. 2 [Brown Dep.] 183:8-20 (describing August 2019 Security & Compliance Program Quarterly Overview and marking it as Brown Exhibit 14); 183:20-221:25 (discussing document)]. The Brown testimony accordingly is not specifically referring to the meaning of text in Def. Ex. 16.

3. August 2019 NIST Scorecard about Pending Migration to Azure AD and Related Notations in Later QRR Presentations

29. The SEC cites a NIST Scorecard included in an August 2019 quarterly risk review ("QRR") presented to management.[31] The SEC has specifically cited a bullet at the top of the slide that states: "Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures."[32] And the SEC has specifically cited the fact that this NIST Scorecard lists a "1" as the "NIST Maturity Score" for "Authentication, Authorization and Identity Management."[33]

SEC Response: Undisputed.

[31] JS ¶177; Def. Ex. 24 (SW-SEC00001497).

[32] Def. Ex. 24 (SW-SEC00001497) at -507.

[33] Def. Ex. 24 (SW-SEC00001497) at -507.

30. Neither the cited bullet nor the "1" score concerns any pervasive failure to implement role-based access controls.[34]

SEC Response: Disputed. The use of the term "concerns any pervasive failure" is conclusory and unsupported by the cited materials. For example, the cited Cline testimony related to the January 2018 "User Access Management" slide deck Defendants submit as Exhibit 10 (SW-SEC00043618). [*See* SEC Ex. 13 [SW-SEC00043618-3630], at -3620 (complete version of Def. Ex. 10)]. It does not relate to the cited bullet or NIST score of "1" referenced in paragraph 30. [*See* Def. Ex. 49 [Cline Dep.] 129:10-20 (marking as Cline Dep. Ex. 6, a January 11, 2018 email and the attached January 2018 User Access Management slide deck), 129:22-143:25 (discussing same document)]. And the cited Brown testimony addresses the movement from Azure model for active directory, generally. Moreover, on its face, the referenced document defines a NIST maturity level score of "1" as meaning "The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objective." [Def. Ex. 24 [SW-SEC0001497], at -1505]. A reasonable juror could understand the plain language of these contemporaneous documents to reflect a pervasive failure, and certainly could do so when considered with the other evidence in the record.

[34] Johnson Decl. ¶¶ 11-15; Def. Ex. 49 (Cline Dep.) 141:14-142:4 ("What that's referencing is our migration into Azure Active Directory."); Def. Ex. 52 (Johnson Dep.) 175:25-176:9 ("I don't stand behind that statement. The statement was in reference to the opportunity to leverage a centralized secret server to store privileged credentials … it was part of a presentation that … had significantly more context."), 181:1-186:12 ("The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company."); Def. Ex. 46 (Brown Dep.) 209:19-210:1 ("At that point in time we had Google and Azure. So consolidating those to make Azure our—our source."); Def. Ex. 45 (Bliss Dep.) 234:3-19 (explaining that score of "1" was "subjective determination" in order to "[g]enerate[] a conversation in this venue.").

31. They are about the efforts that were ongoing at this time to improve the company's access management processes through centralized IAM and PAM tooling, including by migrating to Azure AD and rolling out Thycotic.[35]

SEC Response: Disputed. Although the document may in part reflect efforts to improve access management, the document's statement, on its face, that a NIST maturity level score of "1" means that "The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objective" could be credited by a reasonable juror over the proffered explanation. [Def. Ex. 24 [SW-SEC0001497], at -1505]. From this, a reasonable juror could choose to credit this as contemporaneous documentation of significant failures with respect to "Authentication, Authorization and Identity Management" and conclude that the bullet stating that "Access and privilege to critical systems / data is inappropriate" does not refer to the Azure AD project, but to a separate problem. [*See id.* at -1507]. This is especially the case because the document, on the same page, has a separate bullet point stating "Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets." [*Id.*] From this, not only could a reasonable juror conclude that the bullet concerning inappropriate access and privilege to critical systems and data refers to something other than the Azure AD project, it is the more reasonable and likely conclusion.

[35] Johnson Decl. ¶ 15; Def. Ex. 52 (Johnson Dep.) 181:1-186:12 ("The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company."); Def. Ex. 46 (Brown Dep.) 209:19-210:1 (explaining "movement to make Azure Active Directory the authoritative only source."); Def. Ex. 45 (Bliss Dep.) 234:3-19.

32. Another bullet on the Scorecard specifically references the Azure AD project, stating: "Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets."[36]

SEC Response: Undisputed.

33. A draft of this Scorecard reflects that the "KPI" (key performance indicator) driving the "1" score was the "[n]umber of assets (mission/business critical) with AD Authentication enabled vs. not enabled)"—*i.e.*, the number of systems that had been integrated with Azure AD to date as part of this project.[37]

SEC Response: Undisputed that the cited document includes the quoted language.

34. Moving from manual to automated processes is a common way that companies mature their cybersecurity controls under the NIST CSF.[38]

SEC Response: Undisputed.

35. The migration to Azure AD was a complex, multi-year project that SolarWinds pursued during the Relevant Period.[39]

SEC Response: Undisputed.

36. The "1" score was intended to convey to management (the audience for NIST Scorecards) that the migration to Azure AD was an important opportunity to mature the

[36] Ex. 24 (SW-SEC00001497) at -507.

[37] Johnson Decl. ¶ 15; Def. Ex. 35 (SW-SEC00623600) at -609.

[38] Def. Ex. 2 (Rattray Rep.) ¶ 154; Def. Ex. 50 (Graff Dep.) 216:22-217:1 (agreeing that "one way a company can mature its controls is by making them more automated and more centralized").

[39] Johnson Decl. ¶ 13; Def. Ex. 59 (Kim Dep.) 275:8-17 (noting that "obviously migrating your identity service to a single service actually takes a very long time").

Company's access management processes but that it was still in progress and needed continued support and resourcing.[40]

SEC Response: Disputed. Paragraph 36 is incomplete, and therefore misleading. While Ms. Johnson testified that the "rationale at the time for why this was a 1 is because there was an opportunity to make an investment" in certain software solutions [SEC Ex. 52 [Johnson Dep.] 183:4-5], on its face, the referenced document states that "access and privilege to crucial systems/data is inappropriate" and defines a NIST maturity level score of "1" as meaning "The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objective." [Def. Ex. 24 [SW-SEC0001497], at -1505-06]. A reasonable juror could choose to credit the plain language of this document with other evidence in the record. rather than Ms. Johnson's post-hoc explanation.

37. The ongoing rollout of Azure AD is also what is referred to in notations the SEC cites from subsequent QRR presentations, including:

a. a note from a November 2019 QRR presentation stating "Pushing forward with AD authentication guidelines for critical mission systems";[41]

[40] Johnson Decl. ¶¶ 13-15; Def. Ex. 49 (Cline Dep.) 141:14-142:4 ("What that's referencing is our migration into Azure Active Directory."); Def. Ex. 52 (Johnson Dep.) 175:25-176:9 ("I don't stand behind that statement. The statement was in reference to the opportunity to leverage a centralized secret server to store privileged credentials … it was part of a presentation that … had significantly more context."), 181:1-186:12 ("The rationale at the time for why this was a 1 is because there was an opportunity to make an investment in Thycotic as a secret server for the entire company, and two, to make the investment in Azure AD as the authoritative source for identity and authorization for the company."); Def. Ex. 46 (Brown Dep.) 209:19-210:1 ("At that point in time we had Google and Azure. So consolidating those to make Azure our—our source."); Def. Ex. 45 (Bliss Dep.) 234:3-19 (explaining that score of "1" was "subjective determination" in order to "[g]enerate[] a conversation in this venue.").

[41] Def. Ex. 28 (SW-SEC00001551) at -552.

b. notes from a March 2020 QRR presentation and May 2020 QRR presentation referencing enforcement of "AD authentication" among improvements being made;[42] and

c. a note from an October 2020 QRR presentation stating "Continue to enable AD Authentication for critical systems."[43]

SEC Response: Disputed. The SEC does not dispute that the cited evidence contains the quoted language in paragraph 37, with the exception of Def. Ex. 28 [SW-SEC00001551], at -1552, which reads "guidelines for mission critical systems" in lieu of "guidelines for critical mission systems." The SEC also does not dispute that the specific quoted language relates to the rollout of Azure AD. The SEC does dispute that other language in these QRRs only refers to the rollout of Azure AD, when the plain language of those documents could be understood by a reasonable juror to have other meanings, including that there were "Significant deficiencies in user access management" [Def. Ex. 37 [SW-SEC00001608], at -1611; Def. Ex. 38 [SW-SEC00001602], at -1605; Def. Ex. 40 [SW-SEC00001582], at -1587].

C. March 2020 Slide about User Access Review for SOX Audit

38. The SEC cites a note in a slide in a March 2020 QRR presentation stating: "Significant deficiencies in user access management."[44]

SEC Response: Undisputed.

[42] Def. Ex. 37 (SW-SEC00001608) at -611; Def. Ex. 38 (SW-SEC00001602) at -605.

[43] Def. Ex. 40 (SW-SEC00001582) at -587.

[44] JS ¶¶181, 197; Def. Ex. 37 (SW-SEC00001608) at -611.

39. This note does not concern any pervasive failure to implement the concept of least-privilege access or role-based access controls.[45]

SEC Response: Disputed. The SEC disputes paragraph 39's use of the term "does not concern any pervasive failure" as conclusory and unsupported by the cited materials. The cited paragraphs from the declaration of Ms. Johnson do not reference the quoted language and only refer to the March 2020 QRR presentation in relation to its note regarding "AD authentication." [Johnson Decl. ¶¶16-18]. In addition, the trier of fact could readily find the cited statements by Ms. Johnson in her testimony to be self-serving, not credible, and contradicted by other evidence, including the continued reference to the plural "significant deficiencies" in multiple later QRR presentations including in May 2020 [SEC Ex. 7 [SW-SEC00001602-1607], at -1605] and October 2020 [SEC Ex. 9 [SW-SEC00001582-1601], at -1587]. A reasonable juror could choose to credit this plain language in the contemporaneous documents instead of Ms. Johnson's post hoc rationalization.

40. The note referred to a mistake made in conducting user access reviews in preparation for the Company's 2020 SOX audit: the reviews were run across the wrong window of time, resulting in a significant number of users being erroneously excluded from the review.[46]

---

[45] Johnson Decl. ¶¶ 16-18; Def. Ex. 46 (Brown Dep.) 237:21-24 (explaining that note "isn't a finding. This is simply a statement."); Def. Ex. 52 (Johnson Dep.) 222:3-223:10 ("That was specifically in response to a user access review … so in user access reviews under SOX controls, you are able to define quarterly what the user community that needs to be audited for, whether or not the access is appropriate and that access has been terminated for people who no longer have acquired that access … What I was calling out … is that our user access reviewer didn't understand … how to define the user access review period … That was caught before external auditors reviewed and the internal audit was rerun.").

[46] Johnson Decl. ¶¶ 23-24; Def. Ex. 52 (Johnson Dep.) 222:6-225:11 ("What I was calling out … is that our user access reviewer didn't understand … how to define the user access review period properly … So there was deficiency in user access population that was used to do the user access review.").

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Ms. Johnson claims it does in her post hoc explanation. And a reasonable juror could credit the contemporaneous statement that that there were "[s]ignificant deficiencies in user access management," to mean that there were significant deficiencies in user access management and also credit the fact that the same statement was made in multiple later QRR presentations including in May 2020 [SEC Ex. 7 [SW-SEC00001602-1607], at -1605] and October 2020 [SEC Ex. 9 [SW-SEC00001582-1601], at -1587] to mean that these significant deficiencies in user access management persisted for many months.

41. The note used "significant deficiencies"—a SOX term—loosely, to refer to this SOX-related issue.[47]

SEC Response: Disputed. Paragraph 41 is conclusory and not supported by the cited evidence. The SEC does not dispute that the term "significant deficiencies" are applied to risks in the SOX audit context, but there is no basis in the cited evidence to support that the term was applied "loosely" in reference to the stated issue. Additionally, a reasonable juror could easily understand the plain language of the contemporaneous document to mean that there were significant deficiencies in user access management, and as reflected in the continued reference to the plural "significant deficiencies" in multiple later QRR presentations including in May 2020 [SEC Ex. 7 [SW-SEC00001602-1607], at -1605] and October 2020 [SEC Ex. 9 [SW-SEC00001582-1601], at -1587].

[47] Johnson Decl. ¶¶ 23-25; Def. Ex. 52 (Johnson Dep.) 222:6-222:17 ("[S]o in user access reviews under SOX controls, you are to define quarterly what the user community that needs to be audited for …"); Campbell Decl. ¶ 4.

42. However, the issue was internally discovered and fixed (by re-running the user access reviews in question) before the completion of the Company's actual SOX audit and did not result in any significant deficiency finding by the Company's auditors.[48]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean that there were significant deficiencies in user access management, and as reflected in the continued reference to the plural "significant deficiencies" in multiple later QRR presentations including in May 2020 [SEC Ex. 7 [SW-SEC00001602-1607], at -1605] and October 2020 [SEC Ex. 9 [SW-SEC00001582-1601], at -1587].

43. The "[s]ignificant deficiencies" note in the March 2020 QRR also appears in later QRRs cited by the SEC and refers to the same one-time problem with how user access reviews were initially conducted in preparation for the 2020 SOX audit. The repetition was simply a result of not changing the slide from one iteration of the QRR to the next, and was not intended to indicate any more extensive or continuing problem the Company had regarding access management.[49]

SEC Response: Disputed. The SEC does not dispute that the "[s]ignificant deficiencies" note appears in later QRRs including in May 2020 [SEC Ex. 7 [SW-SEC00001602-1607], at -1605] and October 2020 [SEC Ex. 9 [SW-SEC00001582-1601], at -1587]. However, the SEC disputes the contention that this was a "one-time problem" on the ground that a reasonable juror could easily understand the plain language of the contemporaneous documents to mean that there

[48] Johnson Decl. ¶ 24; Def. Ex. 52 (Johnson Dep.) 222:6-225:11, 226:3-15 ("The issue was remediated once detected [sic]—all of the teams had to rerun their user access reviews. It was remediated before the external audit").

[49] JS ¶¶182-83; 198; Def. Ex. 39 (SW-SEC00148267) at -270; Def. Ex. 38 (SW-SEC00001602) at -605; Def. Ex. 40 (SW-SEC00001582) at -587; Campbell Decl. ¶¶ 10-12; Johnson Decl. ¶ 25.

were significant deficiencies in user access management and that the inclusion of the term in multiple documents meant that the significant deficiencies persisted for many months.

D. "Preliminary Review" Relating to FedRAMP Certification

44. The SEC cites three emails from June, August, and September 2019 attaching a spreadsheet described as "a preliminary review of the 325 FedRAMP Moderate controls," which assessed "what resources are needed for a FedRamp effort" in connection "with the upcoming 2020 budget cycle."[50]

SEC Response: Undisputed.

45. The emails were sent, and the spreadsheet was prepared, by Kellie Pierce, a program manager at SolarWinds who worked under Rani Johnson and Tim Brown.[51]

SEC Response: Disputed. It is undisputed that Kellie Pierce sent the referenced e-mails. The SEC disputes paragraph 45 to the extent it does not accurately describe Ms. Pierce's role with respect to the documents at issue. Ms. Pierce testified that she played a "coordination role" with respect to the FedRAMP control spreadsheet, such that she "downloaded this on the Excel document, the FedRAMP criteria," would request and receive input from the relevant product managers with "more technical expertise than [Ms. Pierce had] on if their product would meet [the applicable FedRAMP control]," those managers "would work within Excel in the same Excel document" and then, based upon that information directly provided by product managers with more technical expertise than Ms. Pierce, she then "scored it with at a red, yellow or green." [Def. Ex. 56 [Pierce Dep.] 47:18-50:23].

---

[50] JS ¶¶174-76; Def. Ex. 22 (SW-SEC00151673) at -673; Def. Ex. 25 (SW-SEC00045356) at -356; Def. Ex. 27 (SW-SEC00218068).

[51] Def. Ex. 56 (Pierce Dep.) 46:19-49:25.

46. "FedRAMP" refers to a type of certification that cloud software must have in order to be sold to the federal government.[52]

SEC Response: Undisputed.

47. FedRAMP certification requires meeting a highly demanding set of controls, which must be established through documentation validated by a third-party assessor.[53]

SEC Response: Disputed. The characterization of FedRAMP as "highly demanding" is not supported by the cited evidence." While the Johnson Declaration uses the terms "highly demanding set of controls," Mr. Graff refers to FedRAMP as a "pretty demanding standard." The SEC does not dispute that FedRAMP is a "demanding" set of controls. [Def. Ex. 50 [Graff Dep.] 241:24-242:1].

48. Ms. Pierce's spreadsheet was prepared as part of a preliminary attempt to estimate how much effort it would require for SolarWinds to achieve FedRAMP certification for its cloud products.[54]

---

[52] Def. Ex. 2 (Rattray Rep.) ¶ 142 ("FedRAMP is a highly demanding set of federal standards that cloud products must meet for the federal government to be able to purchase them."); Johnson Decl. ¶¶ 19-20; Def. Ex. 52 (Johnson Dep.) 203:1-9 ("[T[hat's one of the very foundational components of [F]edRAMP readiness, is that the access to the information systems that are being provided to the U.S. federal government.").

[53] Johnson Decl. ¶ 20; Def. Ex. 50 (Graff Dep.) 241:24-242:1 (agreeing that FedRAMP "is a pretty demanding standard for companies to meet"); Def. Ex. 52 (Johnson Dep.) 194:19-196:2 ("It was a very cursory collection of data … because the formality and the requirement of leveraging a third-party assessment organization or a [third-party auditing organization] for [F]edRAMP is very expensive and you have to create years—at least a year of reporting documentation. … What's more, the—there was … a hypothesis on Kellie's part and certainly mine because she and I have run programs before to prepare companies for product certifications."); Def. Ex. 56 (Pierce Dep.) 125:19-23.

[54] Def. Ex. 56 (Pierce Dep.) 48:3-5 (explaining that this was "a preliminary, very beginning, like, quick and dirty-type evaluation to see if the company wanted to invest in FedRAMP certification"); Def. Ex. 52 (Johnson Dep.) 194:13-16 ("This was a preliminary reaction to a request to make an investment in [F]edRAMP readiness for products that did not have a strong business justification."); Def. Ex. 45 (Bliss Dep.) 186:2-5 (explaining that the objective was to do a "quick, cursory, preliminary review as to how much do we think this is going to cost us? How much effort needs to go into this?"), 186:8-14 (explaining Ms. Pierce was "more or less spitballing" to create a budget estimate); Johnson Decl. ¶¶ 21-22.

SEC Response: Disputed. The SEC objects to the reference to "Ms. Pierce's spreadsheet" to the extent that Ms. Pierce did not draft, but instead played a coordination role in compiling information from various product managers with more technical expertise than Ms. Pierce who directly drafted information into the spreadsheet, as discussed in connection with the SEC's objection to paragraph 45. The SEC otherwise does not dispute paragraph 48 for the purposes of Defendants' motion.

49. Ms. Pierce's takeaway from the preliminary review was that it would take a moderate to significant level of effort to implement most of the FedRAMP controls.[55]

SEC Response: Undisputed.

50. Ms. Pierce's preliminary review was not about whether SolarWinds had implemented the policies described in the Security Statement.[56]

SEC Response: Disputed. The SEC agrees it was not the primary goal of the FedRAMP assessment to determine whether SolarWinds had implemented the policies described in the Security Statement. But some of the specific sub-parts of the FedRAMP assessment did directly examine some of the same precise issues outlined in the Security Statement, as is apparent from the plain language of the contemporaneous documents. [*See, e.g.*, SEC Ex. 63 [Pierce Dep.] 62:18-75:18 (addressing specific controls in Def. Ex. 22 [SW-SEC00151673], including Entry 19 at Pierce Dep. 67:19-70:22 ("organization restricts privileged accounts on the information systems to... organization defined personnel or roles"); Entry 37, 70:25-72:9 ("company does not have a policy on nonnetwork devices connecting to the network"); Entry 38, 72:11-74:2 ("access control for

[55] Johnson Decl. ¶ 22; Def. Ex. 52 (Johnson Dep.) 187:1-203:24 (confirming that the cost of achieving FedRAMP certification would exceed any benefits to SolarWinds).

[56] Def. Ex. 52 (Johnson Dep.) 192:10-18 ("Kellie's ask is to provide a summary of level of effort to prepare for [F]edRAMP readiness that is two years out. It's not an assessment of alignment with controls.").

mobile devices"); and Entry 42, 74:6-75:16 (authorized vs. unauthorized user definitions and policies))]. Therefore, it is misleading (and certainly not undisputed) to say that the FedRAMP assessment was not about the Security Statement policies.

51. The Security Statement says nothing about whether SolarWinds had FedRAMP controls in place.[57]

SEC Response: Disputed. The SEC does not dispute that the term "FedRAMP" does not appear in the Security Statement. However, as described in the SEC's response to paragraph 50, above, some of the controls from NIST 800-53 (which is commonly used to determine FedRAMP compliance) are mirrored almost exactly in the Security Statement [*Compare* Def. Ex. 22 [SW-SEC00151673], at Entry 19 ("organization restricts privileged accounts on the information systems to assignment organization defined personnel or roles") *with* Def. Ex. 1 at 3 ("[r]ole based access controls are implemented for access to information systems"); Def. Ex. 22 [SW-SEC00151673], at Entry 38 ("The organization employs [full-device encryption or container encryption] to protect the confidentiality and integrity of information") *with* Ex. 1 at 2 ("Operational Security...Data Protection...We monitor the changing cryptographic landscape closely and work to upgrade our products to respond to new cryptographic weaknesses as they are discovered..."); Def. Ex. 22 [SW-SEC00151673], at Entry 18 ("The organization requires that users of information system accounts, or roles, with access to...organization-defined security functions or security-relevant information**...**use non-privileged accounts or roles, when accessing nonsecurity functions. authorized vs. unauthorized user definitions and policies.") *with* Def. Ex. 1 at 3 ("[a]ccess controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis")].

[57] Def. Ex. 1 (Security Statement).

52. FedRAMP controls are much more extensive and demanding than the policies described in the Security Statement, including with respect to access controls.[58]

SEC Response: Undisputed. It is also undisputed that, as reflected in the SEC's response to paragraph 51, there are areas of overlap between policies described in the Security Statement and the NIST 800-53 controls used to determine compliance with FedRAMP.

53. FedRAMP controls also generally focus on the security of the cloud products being certified rather than the vendor's cybersecurity program more broadly.[59]

SEC Response: Disputed. Paragraph 53 is vague, ambiguous, conclusory, and not supported by fact witness or documentary evidence. For example, it is unclear how the categorization of controls categorized by particular terms (*i.e.*, "Process," "Product," or "People") supports the conclusion that FedRAMP controls relate to particular products in lieu of "the vendor's cybersecurity program more broadly." [*See* Def. Ex. 22 [SW-SEC00151673], at Column J]. And even if the overall focus of FedRAMP controls is on the security of the products, some clearly directly relate to the organization's overall cybersecurity posture. [*See, e.g.*, Def. Ex. 22 [SW-SEC00151673], at Entry 2 ("The organization...[i]dentifies and selects the following types of information system accounts to support organizational missions/business functions...[and] [a]uthorizes access to the information system based on: (1) A valid access authorization; (2)

[58] *Compare* Def. Ex. 22 (SW-SEC00151673) at pdf p. 5-9 (excerpt of spreadsheet of FedRAMP controls setting forth 45 detailed controls relating to access controls, spanning five pages in small font), *with* Def. Ex. 1 (Security Statement) at 3 (short section describing basic role-based access controls); Ex. 2 (Rattray Rep.) ¶ 145; *see also* Def. Ex. 50 (Graff Dep.) 241:24-242:1 ("Q. And you're aware Fed Ramp is a pretty demanding standard for companies to meet? A. Yes, I'd agree.").

[59] Def. Ex. 2 (Rattray Rep.) ¶¶ 142, 145 ("[M]any of the requirements relate to access controls on the cloud product at issue rather than access controls on SolarWinds' network."); Def. Ex. 22 (SW-SEC00151673) at pdf p. 5-9, column J (containing Ms. Pierce's categorization of each control as either relating to "Process," "Product," or "People," with most categorized as "Product"); Def. Ex. 50 (Graff Dep.) 242:2-6 ("Q. … [T]he certification is for particular cloud products, right, that's what Fed Ramp is for? You have to have that certification to sell a cloud product to the federal government? A. Yes, that's right.").

Intended system usage; and other attributes as required by the organization or associated missions/business functions.")].

54. For example, many FedRAMP controls specifically reference the term "information system"—which is a reference to the cloud product being certified and used by the federal government, rather than the vendor's corporate network.[60]

SEC Response: Disputed. This paragraph selectively quotes the FedRAMP assessment in a misleading manner. While some of the controls in that document refer to assessments of "product" and "information system", others refer to "organization" and "process" which relate to an assessment of the organization's overall cybersecurity posture. [*See, e.g.,* Def. Ex. 22 [SW-SEC00151673], at Entry 1, identified in Column J as "Process" ("The organization: a. Develops, documents and disseminates to [personnel]...An access control policy...[and] Procedures to facilitate the implementation of the access control policy and associated access controls..."); Def. Ex. 22 [SW-SEC00151673], at Entry 2, identified in Column J as "Process" ("The organization ... [i]dentifies and selects the following types of information system accounts to support organizational missions/business functions...[and] [a]uthorizes access to the information system based on: (1) A valid access authorization; (2) Intended system usage; and other attributes as required by the organization or associated missions/business functions.")]. Additionally, this paragraph is vague, ambiguous, conclusory, and not supported by fact witness or documentary evidence. For example, the cited testimony by Mr. Graff is limited to responses regarding a

[60] Def. Ex. 22 (SW-SEC00151673) at pdf p. 7, line 23 (FedRAMP control requiring that "the information system" display a banner at logon advising users that they "are accessing a U.S. government information system"); Def. Ex. 50 (Graff Dep.) 246:20-247:8 ("So the information system being referred to here would be the cloud product that is being sold, which needs to inform users of that product that they're accessing a U.S. government system? A. That's a—that's a reasonable interpretation. ... Q. So it's possible that when you have a number of controls in here to talk about what the information system has to do, it's not talking about SolarWinds network or the organization as a whole, but whatever cloud product is being evaluated for Fed Ramp purposes? A. There's one of them that might well qualify that way.").

"reasonable interpretation" and agreement that "There's one of them [*i.e.*, a reference to an "information system"] that might well qualify that way [*i.e.*, a cloud product being evaluated]." [Def. Ex. 50 [Graff Dep.] 246:20-247:8].

55. Therefore, Ms. Pierce's conclusion that many FedRAMP controls were not in place at the Company does not imply that the representations in the Security Statement were untrue.[61]

SEC Response: Disputed. Paragraph 55 is conclusory and not supported by fact witness or documentary evidence. The only citation for this conclusory statement is from an expert declaration that itself does not support the statement. By contrast, as detailed in the SEC's response to paragraph 54, a number of the FedRAMP controls refer to "organization" and "process," which relate to an assessment of the organization's overall cybersecurity posture. Among other findings, the FedRAMP spreadsheet includes assessments stating: "The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]" [Def. Ex. 22 [SW-SEC00151673], at Entry 17] for which Ms. Pierce's comment was "[w]e have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products." [*Id.*]. Another assessment stated "[t]he organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]," [*id.* at Entry 19] for which Ms. Pierce's comment was, again, "[w]e have no explicit authorization policy, nor is this documented that I am aware of for the company or individual products." [*Id.*] A reasonable jury could conclude from these assessments that corresponding representations in the Security Statement regarding access controls were untrue.

[61] Def. Ex. 2 (Rattray Rep.) ¶ 145.

56. In any event, Ms. Pierce's preliminary review was not a reliable assessment even with respect to FedRAMP controls.[62]

SEC Response: Disputed. A reasonable juror could conclude from the face of the document and the fact that versions of it were emailed to senior leaders such as Ms. Johnson and Mr. Brown on multiple occasions across paragraph 56 is vague and ambiguous. Further, as discussed above in connection with the SEC's objection to paragraph 45, Ms. Pierce played a coordination role in compiling information from various product managers that directly input that information into the assessment spreadsheet [*see* Def. Ex. 56 [Pierce Dep.] 47:18-48:3, 48:15-50:23], and accordingly did not consist exclusively of her own review of applicable FedRAMP controls. That the jury could credit these assessments as reliable is also supported by the fact that SolarWinds personnel who "performed an audit against the NIST800-53" controls in April 2021 similarly concluded that, "about 40% of the baseline controls within NIST [800-53] were met or partially met within the policies reviewed." [Def. Ex. 41 [SW-SEC00185450], at -8450-51].

57. Ms. Pierce was asked to conduct the preliminary review not as a security exercise, but as a budgeting exercise.[63]

SEC Response: Disputed. Paragraph 57's description of the FedRAMP review coordinated by Ms. Pierce as "preliminary" is incomplete and therefore misleading. The review proceeded through a period of several months and involved multiple updates to senior SolarWinds

---

[62] Def. Ex. 56 (Pierce Dep.) 21:17-18 ("I'm not a technical person."), 47:16-17 ("I'm also not a FedRAMP expert. So I'm not 100 percent sure."), 125:19-23 (agreeing she did not "have a good technical understanding of what [the] language in the [FedRAMP] technical controls actually meant"); Def. Ex. 52 (Johnson Dep.) 192:10-18 ("Kellie is not an auditor and has no expertise in this particular area."), 194:12-196:3; Johnson Decl. ¶¶ 21-22.

[63] Johnson Decl. ¶ 22; Def. Ex. 2 (Rattray Rep.) ¶ 142; Def. Ex. 56 (Pierce Dep.) 75:21-76:11 (identifying Ex. 27 (SW-SEC00218068) as "a quantified estimate for the amount of budget we would need if we wanted to move forward with the FedRAMP certification.").

personnel. For example, the three versions of the review spreadsheet (compiled in June, August, and September of 2019 [Def. Ex. 22 [SW-SEC00151673]; Def. Ex. 25 [SW-SEC00045356]; Def. Ex. 27 [SW-SEC00218068], respectively]) were sent to senior personnel such as Mr. Brown and Ms. Johnson and consisted of multiple substantive tabs of data including a review of the implementation status of 325 FedRAMP controls. [*Id.*] A reasonable jury could infer from the extensive content of the documents, months of preparation, and that versions were sent to senior personnel such as Mr. Brown and Ms. Johnson [*see id.*], that this was not a "preliminary" assessment.

58. SolarWinds' cloud software business line wanted to be able to sell its products to the federal government.[64]

SEC Response: Undisputed.

59. Rani Johnson, SolarWinds' Chief Information Officer, did not believe the benefit of being able to sell the federal government SolarWinds' cloud products—which comprised a small portion of SolarWinds' overall business—would be worth the effort required to achieve FedRAMP certification for the products.[65]

SEC Response: Undisputed.

---

[64] Def. Ex. 45 (Bliss Dep.) 184:20-186:14 ("And as we looked at the cloud products, the question became, what do we need to sell those products to our customer base of which some of that was government customers?").

[65] Def. Ex. 52 (Johnson Dep.) 194:19-196:2 ("The reality that these products don't have the U.S.-based staffing infrastructure [required under FedRAMP] means that we knew that we would … this would be too [expensive] of an effort. So this was a very cursory, very preliminary [stab] at [showing] this is gonna cost too much and not going to be worth the effort in this time frame."); Def. Ex. 45 (Bliss Dep.) 35:4-13 (describing cloud product line as "a very small business group"); Johnson Decl. ¶ 22.

60. So Ms. Johnson asked Ms. Pierce to do a "very cursory" review of FedRAMP controls to come up with a rough estimate of the effort required.[66]

SEC Response: Disputed. The SEC does not dispute that Ms. Johnson testified to the request to Ms. Pierce was that of a "very cursory" review, which Ms. Pierce coordinated by working with product managers, relying on their technical expertise and compiling their responses. [Def. Ex. 56 [Pierce Dep.] 48:15-50:23]. However, the SEC disputes the description of the assessment performed as cursory and refers to the documents compiled by Ms. Pierce in connection therewith. [*See, e.g.*, Def. Ex. 22 [SW-SEC00151673]]. That document is an excel workbook containing ten separate worksheets. Even just the worksheet that has been focused on the most during this litigation, the "Moderate Baseline Controls" sheet has more than 300 rows, with information in more than a dozen columns, reflecting comments from multiple SolarWinds employees, including color coded notes and findings. A jury could view this document, and from its face, determine that it was not a "cursory" effort.

61. Ms. Pierce was a program manager who worked under Ms. Johnson, whose entire role at the company was a coordination role.[67]

SEC Response: Undisputed.

---

[66] Def. Ex. 52 (Johnson Dep.) 194:13-196:2 ("The ask here is truly to do a level-of-effort estimate around how much work we need to prepare to create the reporting documentation to ready those assets for [F]edRAMP so we can—say, if this cost 2 million, how much in sales is there to potentially justify this investment. … So this was a very cursory, very preliminary [stab] at this is gonna cost too much and not going to be worth the effort in this time frame."), 202:18-21 ("So my conversations with her were about how much effort to spend because we had a hypothesis that the answer would be the company would not make this investment."); Def. Ex. 56 (Pierce Dep.) 47:18-48:5 ("Q. And what was your involvement in the—assessing FedRAMP moderate controls, if any? A. Again, a coordination role … . ").

[67] Def. Ex. 56 (Pierce Dep.) 87:10-11 ("Similar to pretty much my entire role at SolarWinds. It would have been a coordination role."), 47:16-48:5; Def. Ex. 45 (Bliss Dep.) 32:20-25.

62. Ms. Pierce did not have technical security expertise.[68]

SEC Response: Undisputed.

63. Ms. Pierce lacked a good understanding of what the language in the FedRAMP controls meant.[69]

SEC Response: Disputed. The SEC does not dispute that the Ms. Pierce is not an expert in FedRAMP controls, but that is a different point than saying Ms. Pierce lacked a good understanding of the language in the document, especially as she was getting input from the relevant product managers with "more technical expertise than [Ms. Pierce had] on if their product would meet [the applicable FedRAMP control]," then "compiled the information" and then, based upon that information "scored it with at a red, yellow or green." [Def. Ex. 56 [Pierce Dep.] 47:18-50:23].

64. In reviewing the FedRAMP controls, Ms. Pierce took "basically [her] best guess" as to whether SolarWinds had them in place.[70]

SEC Response: Disputed. The SEC does not dispute that Ms. Pierce testified that the entries were "basically my best guess," [Def. Ex. 56 [Pierce Dep.] 60:18-19], however the SEC notes that Ms. Pierce received input from the relevant product managers with "more technical expertise than [Ms. Pierce had] on if their product would meet [the applicable FedRAMP control]," "compiled the information" and then, based upon that information "scored it with at a red, yellow

---

[68] Def. Ex. 56 (Pierce Dep.) 21:17-18, 28:18-19 ("As I stated before, I'm not a technical person."); Def. Ex. 57 (Pierce Inv. Vol. I) 176:23-24 ("I would coordinate the reports, but I'm not a technical person … ."), 181:21 ("As I stated earlier I'm not highly technical … ."); Def. Ex. 45 (Bliss Dep.) 32:20-25 ("Kellie's role was more to make sure that the trains were running on time, that notes were taken accordingly, that materials were produced. She wasn't a technical resource."); Johnson Decl. ¶ 21.

[69] Def. Ex. 56 (Pierce Dep.) 47:16-17 ("I'm also not a FedRAMP expert."); Def. Ex. 52 (Johnson Dep.) 192:14-15 ("Kellie is not an auditor and has no expertise in this particular area").

[70] Def. Ex. 56 (Pierce Dep.) 28:13-25, 60:10-19.

or green." [Def. Ex. 56 [Pierce Dep.] 47:18-50:23]. A jury could therefore reasonably conclude that document reflected more than Ms. Pierce's best guess.

65. She based her guesses on reading the language in each control and seeing if she recalled seeing similar language in SolarWinds policy documentation she had reviewed in the past, through coordinating SOC-2 audits the Company had completed.[71]

SEC Response: Disputed. The SEC does not dispute that this describes part of the steps that Ms. Pierce took, but disputes that her answers were just guesses and disputes that this was the entirety of the steps that she took for the reasons set forth in the SEC's response to paragraph 64.

66. Ms. Pierce's comments in her preliminary review were never validated by anyone else for accuracy.[72]

SEC Response: Disputed. Paragraph 66 does not accurately reflect Ms. Pierce's testimony. Ms. Pierce testified that she "did not know" if anyone reviewed her notes for accuracy, and did not expect that anyone had. [Def. Ex. 56 [Pierce Dep.] 127:19-24]. Ms. Pierce did email versions of the FedRAMP review to her senior managers—including Ms. Johnson and Tim Brown—on at least two occasions. [Def. Ex. 25 [SW-SEC00045356]; Def. Ex. 27 [SW-SEC00218068]]. Additionally, Ms. Pierce's comments were based in part on discussions with relevant persons with technical expertise, which implies a degree of vetting. [Def. Ex. 56 [Pierce Dep.] 47:20-50:23; s*ee also* response to paragraph 64].

---

[71] Def. Ex. 56 (Pierce Dep.) 49:8-17, 55:3-56:1 ("Again, this was a very preliminary, you know, just a request that we—that we got to do turnaround pretty quickly, so I made my best guess based on what—what I had seen in the SOC 2 or the ISO 27001 audits."), 124:22-125:18 ("Q. Did you rely on anything other than your memory of those policies based on your limited experience coordinating SOC 2 and ISO audits? A. No, I did not.").

[72] Def. Ex. 56 (Pierce Dep.) 50:8-17; Def. Ex. 52 (Johnson Dep.) 194:12-195:10, 196:16-23.

67. The only FedRAMP control evaluated in the preliminary review that resembles a representation made in the Security Statement concerning access controls is a control stating: "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."[73]

SEC Response: Disputed. Paragraph 67 inaccurately states that there was "only" a single FedRAMP control evaluated that "resembles" a representation made in the Security Statements. This ignores that there are others, including "The organization restricts privileged accounts on the information systems to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]" [Def. Ex. 22 [SW-SEC00151673], at Entry 17] for which Pierce's comment was "[w]e have no explicit authorization policy, nor is this document[ed] that I am aware of, for the company or individual products." [*Id.*; *see also* SEC. Ex. 63 [Pierce Dep.] 69:6-75:16].

68. In the spreadsheet she prepared, Ms. Pierce marked this as a control SolarWinds "may have" in place and placed a comment stating: "This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed."[74]

SEC Response: Undisputed.

69. The comment was inaccurate, as SolarWinds' systems had been audited previously against the principle of least privilege.[75]

---

[73] Def. Ex. 2 (Rattray Rep.) ¶ 146; Def. Ex. 22 (SW-SEC00151673) at pdf p. 7, line 16.

[74] Def. Ex. 22 (SW-SEC00151673) at pdf p. 7, line 16.

[75] Def. Ex. 2 (Rattray Rep.) ¶ 147 ("SolarWinds *did* audit its compliance with the least privilege principle, through the user access reviews that it regularly conducted, which looked specifically at what level of privilege each user in the company had."); Def. Ex. 3 (Graff Rep.) ¶¶ 61, 97 & n.180 (referencing certain audits for least privilege).

SEC Response: Disputed. The SEC disputes paragraph 69 because it implies that all SolarWinds systems had been audited against the principle of least privilege. This is not supported by the cited materials. For example, the cited portion of the Graff Report used to support this paragraph refers to investigative testimony of Eric Quitugua that "We identified… as part of our internal audits and checks that *not all systems* which were under IT control were following best practice." [Def. Ex. 3 [Graff. Rep.] ¶61 (quoting Quitugua Inv. Vol. II 280:13-281:4) (emphasis added)].

E. Engineer's Concerns about Employees Using Personal Laptops on VPN

70. The SEC cites emails in which Róbert Krajčír, a network engineer, conveyed concerns he had about the fact that SolarWinds employees and contractors could use their personal laptops to remotely log into their SolarWinds accounts through the Company's VPN—a practice commonly referred to as "Bring Your Own Device" or "BYOD."[76]

SEC Response: Disputed. The SEC does not dispute that it cites these emails, but disputes Defendants' short summary of the emails as incomplete and therefore misleading. Among other things, in his email, Mr. Krajcir writes, in red font, about the "risk we are facing," including that "[a]nyone with AD credentials can access [SolarWinds] corporate wifi or corporate VPN from ANY device" and that "[w]hile on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late," providing examples of "easily download[ing] any content without being detected by NetScope" and "compromis[ing] entire network by spreading malware." [Def. Ex. 15 [SW-SEC00594395], at -4396].

[76] JS ¶¶166, 168-69, 180; Def. Ex. 14 (SW-SEC00031653) at -657; Def. Ex. 15 (SW-SEC00594395) at -395; Def. Ex. 34 (SW-SEC00666779) at -779; Krajčír Decl. ¶ 5.

71. Mr. Krajčír's concerns regarding BYOD did not concern role-based access controls or the principle of least privilege.[77]

SEC Response: Disputed. The emails cited in paragraph 70 themselves refer to role-based restrictions, including a proposed group for users whose "profile[s] should have stricter policy and tier access should be limited" and "separate groups for vendors, contractors etc., depending on how many levels of restriction will be required." [Def. Ex. 14 [SW-SEC00031653], at -1656]. Further, in a PowerPoint presentation entitled "BYOD solution, Machine certificate authentication that Mr. Krajcir attached to an August 30, 2018 email cited in paragraph 70, Mr. Krajcir wrote on a slide titled "Implementing Certificates" that SolarWinds had to "[m]anage user admin rights" that he described as being "[a]t this time basically unlimited." [SEC Ex. 15 [SW-SEC00031653-1668], at -1662 (whereas Def. Ex. 14 consists of the August 19, 2018 email and cover slide of the presentation attached thereto, SEC Ex. 15 incorporates the full slide presentation, including the quoted text)]. A reasonable juror could easily understand the plain language of these contemporaneous documents to mean that Mr. Krajcir's concerns related to role-based access controls and a failure by SolarWinds to adhere to the principle of least privilege.

72. Mr. Krajčír's concerns instead were about SolarWinds' ability to monitor user personal devices connected to the network—for example, to monitor whether the devices might be infected with malware.[78]

SEC Response: Disputed. It is incomplete and therefore misleading. The referenced testimony from Mr. Cline is made in response to a single proposal by Mr. Krajcir: "Q…He

[77] Krajčír Decl. ¶ 6; Def. Ex. 49 (Cline Dep.) 183:18-184:9 (explaining that Krajčír was "referring to attempting to implement certificates on devices joining our VPN to remove the potential for unmanaged devices.").

[78] Krajčír Decl. ¶¶ 7-8; Def. Ex. 49 (Cline Dep.) 191:9-25, 192:18-197:3 ("So to be clear, he's talking about administrative rights on your local device.").

suggests: Trim down user admin rights so that they won't be able to export certificates on their PC.…What has been done to reduce admin rights as of August 2018? What had been done to reduce admin rights?... A: So to be clear, he's talking about administrative rights on your local device." [Def. Ex. 49 [Cline Dep.] 192:20-193:5]. Further, as reflected by Mr. Krajcir's own e-mails and August 2018 presentation, his concerns extended beyond the ability to monitor user personal devices and to, as he stated, the ability of users to "do[] anything to [SWI's] core systems" including "[a]ccess resources (code, databases…)," and "[w]orst-case scenarios for the company" in which "there will be major reputation and financial loss to the company." [SEC Ex. 15 [SW-SEC00031653-1668], at -1662].

73. The Security Statement section on role-based access controls does not say anything about the Company's BYOD policies or whether users were required to connect to the Company's network from a company-managed device.[79]

SEC Response: Undisputed.

F. August 2017 Budget Request and October 2018 Draft Update

74. The SEC cites a slide deck for SolarWinds' Monthly IT Leadership Meeting in August 2017.[80]

SEC Response: Undisputed.

75. The slide deck includes a $660,000 budget request from Mr. Brown—earmarked for additional personnel, security tools, and training for employees.[81]

SEC Response: Undisputed.

---

[79] Krajčír Decl. ¶¶ 4, 6; Def. Ex. 1 (Security Statement) at 3.

[80] JS ¶¶159-60; Def. Ex. 7 (SW-SEC00259782) at -787-88.

[81] Def. Ex. 7 (SW-SEC00259782) at -788.

76. Next to the budget request, under the heading "Risks of Non-Investment," Mr. Brown included a bullet point stating: "Current state of security leaves us in a very vulnerable state for our critical assets."[82]

SEC Response: Undisputed that the cited document contains the language quoted therein. It is also undisputed that the term "vulnerable state" as it appears in the document is bolded and italicized, and that the quoted bullet also contains the additional following language: "A compromise of these assets would ***damage our reputation and impact us financially.***" [Def. Ex. 7 [SW-SEC00259782], at -9788 (emphasis in original)]. It is also undisputed that the same slide includes the following language: "Lack of cyber hygiene leaves us ***open to being a target*** of opportunity and a compromise will create downtime and lost revenue," and "Without training our **employees** will continue to be one of our ***biggest risks."*** [*Id*. (emphasis in original)].

77. This language was merely hyperbole intended to underscore the importance of investing in cybersecurity and increase the likelihood his budget request would be granted.[83]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Mr. Brown claims for the first time in his post-deposition declaration. Issues of witness credibility are for a jury, and it is axiomatic that a witness's demeanor while testifying live at trial is part of the evidence. Indeed, Mr. Brown's post-hoc explanation of this language as "hyperbole" is, at core, an attack on the credibility and accuracy of the contemporaneous document and presents a quintessential question of fact for a jury to determine. Mr. Brown's explanation is contradicted by the plain language of the cited material, which as noted in the SEC's response to paragraph 76, was emphasized in the

[82] Def. Ex. 7 (SW-SEC00259782) at -788.

[83] Brown Decl. ¶¶ 3-5; Def. Ex. 46 (Brown Dep.) 157:10-13, 160:6-7.

original. That language was further repeated by Mr. Brown in later presentation materials through at least October 2018. [*See, e.g.,* Def. Ex. 8 [SW-SEC00337355], at -7360; Def. Ex. 9 [SW-SEC00262716], at -2743; Def. Ex. 19 [SW-SEC00313350], at –3361; s*ee also* www.merriam-webster.com/dictionary/hyperbole ("extravagant exaggeration (such as 'mile-high ice cream cones')") (last visited June 5, 2025)].

78. The language was likewise understood by the audience for the presentation to be jargon Mr. Brown was using to make a business case for the budget request, as opposed to a specific factual finding.[84]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Defendants now claim, as detailed in the SEC's response to paragraph 77. Additionally, to the extent that any witness purports to testify to what another person understood the presentation to mean, that testimony is inadmissible speculation that cannot serve as the basis for an undisputed fact and the SEC objects on that basis. Finally, as with paragraph 77, the testimony on which Defendants now rely, such as Ms. Johnson's post-hoc testimony that the document "is not accurate" presents a quintessential question of fact of whether the jury should credit the contemporaneous documents or the explanations provided for those documents after this litigation commenced. [*See* SEC Ex. 52 [Johnson Dep.] 141:7-142:10].

[84] Def. Ex. 45 (Bliss Dep.) 216:20-217:8 ("My understanding of that statement, first, is that it was attached originally to a budget request being made. So as with any budget request, there's a certain amount of hyperbole that's introduced…."); Def. Ex. 52 (Johnson Dep.) 139:2-11 ("I don't know what Tim was intending by these statements. However, the purpose of the 2017 document … was to make a business case. Business case justifications are generally jargon or summarized nonprecise language to make a point to make investment."), 141:7-142:10 ("The statements he was making in a slide deck to his boss and to make a business justification weren't a statement of status or qualified in any way. It was merely meant to make a business justification. … [The language] is not accurate.").

79. The language was not intended to convey that SolarWinds was pervasively failing to implement role-based access controls (or any other practices described in the Security Statement).[85]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Mr. Brown claims it does, as detailed in the SEC's responses to paragraphs 77 and 78. Specifically, the testimony on which Defendants now rely, such as Ms. Johnson's post-hoc testimony that the document's language is "not intended to make a statement on the status of security; it's to make a request to invest," [SEC Ex. 52 [Johnson Dep.] 141:12-14], presents a quintessential question of fact of whether the jury should credit the contemporaneous documents or the explanations provided for those documents after this litigation commenced. Indeed, a jury could accept that the purpose of the language was "to make a request to invest," and still conclude that Mr. Brown conveyed an accurate description of the state of cybersecurity at SolarWinds at the time, underscoring the need for investment.

80. The SEC cites slide decks from September 2017 and December 2017 that include a copy of Mr. Brown's budget request from the August 2017 presentation, containing the same language.[86]

SEC Response: Disputed. Although the SEC does not dispute that it cites the September 2017 and December 2017 slide decks and that both contain the language "Current state of security

---

[85] Brown Decl. ¶¶ 3-5, 21; Def. Ex. 46 (Brown Dep.) 157:2-15 (explaining that the language was part of an "attempt[] to support my budget request"); Def. Ex. 45 (Bliss Dep.) 220:4-221:5 ("I do not think this is a factual finding."); Def. Ex. 52 (Johnson Dep.) 139:13-21 ("It's not intended to make a statement on the status of security; it's to make a request to invest."), 141:12-14 ("That statement is imprecise and not accurately reflecting—it is a business case justification, like, of a problem statement.").

[86] JS ¶¶161-64, 172-73; Def. Ex. 8 (SW-SEC00337355) at -360; Def. Ex. 9 (SW-SEC00262716) at -743.

leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and [impact us] financially," the SEC disputes that these "copy" all the language because the "Overall Budget Request" portion of the relevant slides in those decks [Def. Ex. 8 [SW-SEC00337355], at -7360 and Def. Ex. 9 [SW-SEC00262716], at -2743, respectively] are not a "copy" of the same budget request from the August 2017 presentation [Def. Ex. 7 [SW-SEC00259782], at -9788] in that they request different total funding amounts (*i.e.*, "$680k + 30% time of 4 Security Champions") than the August 2017 presentation ("$660K").

81. The repetition of the budget request in these slide decks is simply a result of the information being copied into similar slide decks—it does not represent any repeated "findings" by Mr. Brown.[87]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Mr. Brown claims it does, as detailed in the SEC's response to paragraphs 77 to 79, and because, as set forth in the SEC's response to paragraph 80, not all of the information on these slides was "copied" into the new slide.

82. The SEC also cites a draft slide deck emailed from Mr. Brown to Rani Johnson on October 29, 2018, titled "Information Security - Risk review October 2018."[88]

SEC Response: Undisputed.

[87] Brown Decl. ¶ 6.

[88] JS ¶173; Def. Ex. 19 (SW-SEC00313350) at -351.

83. Mr. Brown stated in the email that the draft included "[a] review of what we asked for last August and a red yellow green status showing how we have done on our initiatives. … We can review in tomorrow but it's a reasonable place to start."[89]

SEC Response: Undisputed.

84. The draft included two copies of Mr. Brown's budget request from August 2017—one as it originally appeared, and a second copy labeled "Updated October 2018 with status," with the font color of some of the language from the original budget request changed to either red, yellow, or green. The language "Current state of security leaves us in a very vulnerable state for our critical assets" was changed to yellow font in the second copy of the slide.[90]

SEC Response: Disputed. It is undisputed that the quoted language in paragraph 84 regarding the current state of security appears in yellow font in the October 2018 slide deck, and that the following language also appears on the same slide: "Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue" (in green font), "We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive" (in red font), and "Without training our employees will continue to be one of our biggest risks" (in red font). However, paragraph 84 is disputed for reasons stated in response to paragraph 80: that the August 2017 budget request in the October 2018 deck is a "cop[y]... as it originally appeared." [*Compare* Def. Ex. 7 [SW-SEC00259782], at 9788 *with* Def. Ex. 19 [SW-SEC00313350], at -3359].

[89] Def. Ex. 19 (SW-SEC00313350) at -350.

[90] Def. Ex. 19 (SW-SEC00313350) at -359, -361.

85. All Mr. Brown meant to convey by yellow font is that improvements had been made since August 2017, but there was still work to be done.[91]

SEC Response: Undisputed.

86. Ms. Johnson's reaction to the draft was that it was "not the way we would formally represent completion or risk" or the "status of initiatives," and thus the draft would not have been finalized in this form (if it was ever finalized).[92]

SEC Response: Disputed. It is undisputed that this was Ms. Johnson's explanation of her reaction in her deposition. However, the language cited by Defendants to support this fact includes a post-hoc explanation by Ms. Johnson that the language in the contemporaneous document was "imprecise." To the extent Defendants are trying to incorporate that post-hoc explanation into this fact, the SEC disputes it as a reasonable juror could choose to credit the plain language of the contemporaneous document over the post-hoc explanation provided a witness (especially one who did not draft the document).

III. DOCUMENTS THE SEC RELIES ON AS TO THE PASSWORD REPRESENTATION

A. March 2018 Slide about Progress on User Account Audit

87. The SEC cites a slide in a draft slide deck attached to an email in March 2018, containing a progress report on a project titled "Enterprise Access Management (Standards &

---

[91] Brown Decl. ¶ 7; Def. Ex. 46 (Brown Dep.) 167:3-168:5 ("[Y]ellow indicates that some of it was done and we could do more ... certain improvements had been done and there were still more to do.").

[92] Def. Ex. 52 (Johnson Dep.) 133:9-134:12 ("This is not the way we would formally represent completion or risk. It is likely why Tim wanted to meet. … The DOIT organization presented monthly status of all initiatives. This is not the format for the presentation of status of initiatives. … And so I would have worked with him to finalize this in a consistent manner with our artifacts."), 139:2-25 ("[T]he purpose of the 2017 document that was updated in 2018 with Tim Brown's color coding was to make a business case. Business case justification are generally jargon or nonprecise language to make a point to make investment."), 140:16-17 ("It's a business case document using nonprecise terms to make the point to invest.").

Audit).” The SEC cites in particular two notations in the lower left corner of the document, under “Issues, Risks & Dependencies,” stating: “Concept of least privilege not followed as a best practice” and “Use of shared accounts throughout internal and external applications.”[93] The SEC cites this same language that was copied into a May 2019 slide deck.[94]

SEC Response: Disputed. It is undisputed that the March 2018 document contains the quoted language. It is also undisputed that the March 2018 slide further states a corresponding “Action[s] Required” of “ID existing permission levels within the enterprise” and “[w]ork with teams to decommission use of shared accounts” [Def. Ex. 13 [SW-SEC00042892], at -2907] with language at the bottom of the slide reading “10/16/2017 Update – Identity management continues to be a concern. Appropriate checks are in place to grant access but audit of access is not consistently implemented.” [Def. Ex. 13 [SW-SEC00042892], at -2907]. It is also undisputed that the May 2019 slide deck contains the language referenced by Defendants, in addition to a further item under the subheading “Issues, Risks & Dependencies” and “Action Required” of, respectively: “Project scope expanded to include SOX compliance requirements” and “Need to assess existing control to ensure alignment with SOX requirements.” [Def. Ex. 26 [SW-SEC00001635], at -1644]. It is also undisputed that this same additional language from the May 2019 slide deck appears in an August 16, 2019 Security & Compliance Program Quarterly Review. [Def. Ex. 24 [SW-SEC00001497], at -1523; *see also* JS ¶178]. However, it is disputed that any language was “copied” as opposed to being independently re-written, as there is no admissible support cited for this assertion. Instead, the cited Campbell Declaration merely contains speculation that the language “appears to have been copied.”

---

[93] JS ¶184; Def. Ex. 13 (SW-SEC00042892) at -907.

[94] JS ¶178: Def. Ex. 26 (SW-SEC00001635) at -644; Campbell Decl. ¶¶ 13-14.

88. This project concerned an audit of user accounts that was conducted in late 2017, approximately a year before the Relevant Period.[95]

SEC Response: Disputed. It is unsupported by the cited evidence. As reflected in the SEC's response to paragraph 87, various versions of the slide were included in decks dated between at least 2017 and 2019, with Ms. Campbell noting in the cited declaration that the May 2019 version of the slide was about "an ongoing project" that "related to our efforts to prepare for our first SOX audit *after our 2018 initial public offering*," and claiming that "most of the work for the project had been completed by early 2019." [Campbell Decl. ¶¶13-14 (emphasis added)].

Further, the cited testimony from Mr. Quitugua does not relate to any version of the slide at issue, but rather to a slide from the March 2018 slide deck (a portion of which SolarWinds produced as Def. Ex. 13) that Mr. Quitugua described as "working through [European Union General Data Protection Regulation] readiness [in 2018] and one of the tasks was to conduct a security assessment and remediation." [Def. Ex. 54 [Quitugua Dep.] 201:11-202:1 (referencing Def. Ex. 13 [SW-SEC00042892-2964], at -2906)]. In addition, the report of Mr. Rattray does not provide any independent or contemporaneous insight into the document, but simply Mr. Rattray's speculative reading thereof (*i.e.*, "the notation could simply have meant... [t]his indicates that the processes *were* generally in place... [t]his also indicates the purpose of the project was to conduct an audit of user access...."). [Def. Ex. 2 [Rattray Rep.] ¶137 (emphasis in original)].

89. The notation "Concept of least privilege not followed as a best practice" refers to the "issue" the audit was looking into—*whether* the concept of least privilege was not being followed as a best practice on the audited systems, as reflected in the project components listed on

[95] Def. Ex. 2 (Rattray Rep.) ¶ 137; Def. Ex. 54 (Quitugua Dep.) 202:13-203:10; Campbell Decl. ¶¶ 13-14.

the other side of the slide (*e.g.*, "Conduct risk audit and risk assessment against privileged and non-privileged user accounts").[96]

SEC Response: Disputed. A reasonable juror could easily understand the plain language of the contemporaneous document to mean something different than what Mr. Quitugua claims it does (as Mr. Quitugua is the only fact witness cited in support of this paragraph), including taking at face value the statement that least privileged was "not followed as a best practice." Indeed, as Mr. Quitugua stated when asked whether this project indicated that the concept of least privilege was not being followed, Mr. Quitugua testified that "that could have very well been raised as a concern," and that, "[a]s part of the assessment, it may have been found that a particular system wasn't following the concept of least privilege." [Def. Ex. 54 [Quitugua Dep.] 218:20-219:24]. Mr. Quitugua also testified that he could not "distinctly recall" whether there were particular instances where the concept of least privilege was not being followed. [Def. Ex. 54 [Quitugua Dep.] 220:2-10]. Thus, the difference between the plain language of the contemporaneous documents and the post-hoc explanation presents a quintessential question of fact for jurors to resolve.

90. As testified by Eric Quitugua, who was the lead for the project listed on the slide, the notation "doesn't indicate" there was any "problem across the organization."[97]

SEC Response: Disputed. The SEC disputes paragraph 90 for the reasons detailed in its response to paragraph 89. Similarly, Ms. Campbell also asserted that the notations "Concept of lease privilege not followed as a best practice" and "Use of shared accounts throughout internal

[96] Def. Ex. 54 (Quitugua Dep.) 219:14-22 ("The issue, risk and dependencies listed here, doesn't indicate that it was a problem across the organization."); Def. Ex. 13 (SW-SEC00042892) at -907; Def. Ex. 2 (Rattray Rep.) ¶ 137.

[97] Def. Ex. 54 (Quitugua Dep.) 219:14-24; Def. Ex. 2 (Rattray Rep.) ¶¶ 138-39.

and external applications" did not refer to any "pervasive" problem that was uncovered as a part of SolarWinds' SOX-related audit work, while at the same time acknowledging in her declaration that she did not know what the notations "were originally intended to refer to." [Campbell Decl. ¶15 [referring to Def. Ex. 26 [SW-SEC00001635], at-1644]]. As with Mr. Quitugua's statements, those by Ms. Campbell contradict the plain words of contemporaneous documents and present a material dispute of fact.

91. "As part of the assessment, it may have been found that a particular system wasn't following the concept of least privilege."[98] But to the extent any non-compliant systems were identified, they would have been remediated as part of the audit. [99]

SEC Response: Disputed. Paragraph 91 is not supported by the cited testimony. Neither of the cited testimonies stand for the proposition that non-compliant systems *would have been* remediated, but rather that there existed procedures to review and fix non-compliant systems. See also the SEC's response to paragraph 89.

92. Another "issue" the audit covered was checking internal and external applications for the use of shared accounts.[100]

SEC Response: Undisputed.

93. Specifically, as Mr. Quitugua explained, the audit was focused on *service accounts*, which are accounts intended for use by an application, rather than individual users. For example,

---

[98] Def. Ex. 54 (Quitugua Dep.) 219:14-24.

[99] Def. Ex. 54 (Quitugua Dep.) 219:14-220:10 ("[W]e do have those kind of defined steps to go through to identify, take in the reports and then address and fix."); Def. Ex. 50 (Graff Dep.) 203:22-204:5 (agreeing that audits are meant "to make sure everything is going well and if there's things that are not going well to identify them for mitigation[.]").

[100] Def. Ex. 55 (Quitugua Inv. Vol. II) 291:25-293:2 (explaining that the intent of the project was "to work with teams to decommission the use of those shared accounts," by first identifying shared accounts and determining if they were needed by the application, and then "rotat[ing] the credentials" for the accounts so "they couldn't be used as shared").

if an application needs to look up information from a database, it may need an account on that database to be able to do so. That account is called a "service account."[101]

SEC Response: Undisputed.

94. Prior to conducting the audit, Mr. Quitugua had discovered instances where service accounts intended for use by an application were being used by individual members of the relevant application team in the course of their work, which was not best practice.[102]

SEC Response: Undisputed. It is also undisputed that Mr. Quitugua testified as to the risks involved in the sharing of service accounts, including that "[t]here's no way for – for teams to identify, you know, who was the individual using that shared credential," which was an access control issue that "needs to be remediated." [Def. Ex. 55 [Quitugua Inv. Vol II] 288:13-22].

95. As part of the audit, Mr. Quitugua undertook an effort to identify any service accounts used in this way and decommission them wherever found.[103]

SEC Response: Undisputed.

96. The slide identifies Q1 2018 as the completion date for the work, which is well before the Relevant Period.[104]

---

[101] Def. Ex. 55 (Quitugua Inv. Vol. II) 289:20-290:21 (explaining that "service accounts" were "used to run automated scripting processes within the business applications"); Def. Ex. 54 (Quitugua Dep.) 221:8-23 (explaining that a "shared account … can be used by a computer to perform its function"); Def. Ex. 2 (Rattray Rep.) ¶ 162.

[102] Def. Ex. 55 (Quitugua Inv. Vol. II) 289:20-290:21 ("What we found was that these service accounts, which were purpose built to run processes, were also being used by, you know, users, and they also knew the credentials, right. So that case, we considered those accounts shared accounts, accounts that users should not have access to … ."); Def. Ex. 2 (Rattray Rep.) ¶¶ 162-63.

[103] Def. Ex. 55 (Quitugua Inv. Vol. II) 291:25-293:2 (explaining that the intent of the project was "to work with teams to decommission the use of those shared accounts," by first identifying shared accounts and determining if they were needed by the application, and then "rotat[ing] the credentials" for the accounts so "they couldn't be used as shared"); Def. Ex. 2 (Rattray Rep.) ¶¶ 162-63.

[104] Def. Ex. 13 (SW-SEC00042892) at -907.

SEC Response: Disputed. Paragraph 96 is incomplete and, therefore, misleading. The slide at issue includes Q1 2018 as the *targeted* completion date for the milestones "Track remediation and map to access control guidelines and standards" and "Document results and establish repeatable security assessment methodology for continuous monitoring," and lists the "Status" of those milestones as "Not Started." [Def. Ex. 13 [SW-SEC00042892], at -2907]. The four milestones prior to those tasks are listed as "in progress" as of March 16, 2018, despite having earlier targeted completion dates. [Def. Ex. 13 [SW-SEC00042892], at -2907].

97. Auditing policies to find and remediate gaps is a means of enforcing those policies.[105]

SEC Response: Undisputed.

98. This audit was part of SolarWinds' efforts to enforce the principle of least privilege and a policy against the use of shared accounts.[106]

SEC Response: Disputed. Paragraph 98 is supported solely by speculation on the part of Mr. Rattray, who testified only as to his personal experience as a former CISO and his general interpretation of the audit without support from contemporaneous documents.

99. In any event, the Security Statement itself does not make any representation that SolarWinds employees never use shared accounts. It merely states that SolarWinds requires that

[105] Def. Ex. 2 (Rattray Rep.) ¶ 171 ("Identifying and remediating discrepancies is what an audit is conducted for … .").

[106] *Id.*; *see also id.* ¶ 130 ("As I know from my experience as a CISO at a large organization, this is what a well-functioning cybersecurity program does on a daily basis: It has general processes in place, but is always on the lookout for specific areas where those processes can be improved."), ¶ 163 ("That is exactly what you would expect a well-functioning cybersecurity program to do in order to *enforce* a policy against sharing of accounts: identify a gap, investigate it further, and remediate it.").

employees be "provisioned with unique account IDs," which was in fact the Company's routine practice.[107]

SEC Response: Disputed. Undisputed that the Security Statement stated: "We require that authorized users be provisioned with unique account IDs." [Def. Ex. 1 [Security Statement], at 3]. The SEC disputes paragraph 99 because a reasonable juror could easily find that it was materially misleading by omission for SolarWinds to state that users were provisioned with unique IDs while omitting all of the information showing that users then shared IDs. *See* Responses to paragraphs 84-96.

B. November 2019 Emails about Developer Access to Billing Data

100. The SEC cites a November 2019 email chain, in which an employee stated that certain software developers "are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop. Solution – Granting the individual logins as requested."[108]

SEC Response: Undisputed. It is also undisputed that the cited document includes the following highlighted language: "The developers are developing in Production as the staging/dev environments are not suitable. Solution – Create a billing RC environment that is the same as production and then pulling access from all Developers," which was described by SolarWinds personnel as activity that needed to "to stop immediately... That is a significant security and Sox [sic] violation." [Def. Ex. 29 [SW-SEC00254254], at -4265].

---

[107] Def. Ex. 1 (Security Statement) at 3; Def. Ex. 2 (Rattray Rep.) ¶ 160 ("The Security Statement does not purport to guarantee that sharing of accounts never occurred at SolarWinds. Instead it merely states that SolarWinds 'require[s] that authorized users be provisioned with unique account IDs.'"), ¶169 (same).

[108] JS ¶186; Def. Ex. 29 (SW-SEC00254254) at -265.

101. The software developers were working on improvements to the billing system used by SolarWinds' Finance Department.[109]

SEC Response: Undisputed.

102. To complete that task, the developers needed access to the billing data.[110]

SEC Response: Undisputed.

103. To access the billing data required having SuperUser access on the relevant billing system.[111]

SEC Response: Disputed. Paragraph 103 is incomplete and therefore misleading. As detailed in the cited document, this was not a "new" procedure as "we were developing billing using production services since the beginning as only production has data to test billing," [Def. Ex. 29 [SW-SEC00254254], at -4265]. However, there was an available solution that did not require giving developers SuperUser access, which was to "create a special 'read-only' level of access that the developers could use." [Def. Ex. 2 [Rattray Rep.] ¶123 (citing Def. Ex. 29 [SW-SEC0025425], at -5255)]. Creating this read-only level of access to billing data "would take approximately 2 weeks." [Def. Ex. 43 [SW-SEC00168780], at Column E].

---

[109] Def. Ex. 29 (SW-SEC00254254) at -258; Def. Ex. 2 (Rattray Rep.) ¶ 122.

[110] Def. Ex. 29 (SW-SEC00254254) at -265 (explaining that "we were developing billing using production services since the beginning as only production has data to test billing"), -264 (explaining it would require engineering effort to obtain "enough test data" without "going to production" for it), -260 (explaining that the issue was "how best to secure access to production data in order to improve our billing systems"); Def. Ex. 2 (Rattray Rep.) ¶ 122; Def. Ex. 50 (Graff Dep.) 161:22-162:2 ("Q. The developers thought they needed [access to] it, right? A. Either the developers or their manager."), 171:16-22 ("Q… . The principle [of role-based access] is employees getting access based on what they need to do for their role. Here there was a determination made that, in order to perform their role, they needed this access at the time. The company was entitled to make that determination, was it not? A. Yes."), 173:8-11 ("There was one specific group of people that needed access, were declared to have needed access, and they were given read-write access using shared log-ins on live production data … ."), 174:1-8 ("Yes, and they needed read access for their jobs. … The company is within its right to make that exception to the role-based access controls.").

[111] Def. Ex. 29 (SW-SEC00254254) at -262-63; Def. Ex. 50 (Graff Dep.) 162:1-2; Def. Ex. 2 (Rattray Rep.) ¶¶ 122-24.

104. Because the developers lacked such access on the system, they initially borrowed the credentials of a different SolarWinds employee with SuperUser access.[112]

SEC Response: Disputed. Paragraph 104 is conclusory and not supported by the cited evidence. The SEC does not dispute that SolarWinds developers borrowed the credentials of a different SolarWinds employee with SuperUser access, however the term "initially" suggests that this practice occurred over a recent time and limited duration. A reasonable juror could easily understand the plain language of the contemporaneous document – *i.e.*, "[a]s far as I know *it's not something new,* we were developing billing using production services *since the beginning* as only production has data to test billing" [Def. Ex. 29 [SW-SEC00254254], at -4265 (emphasis added)] to mean that the sharing of logins to access billing data to which the developers did not otherwise have access was a long-established practice at SolarWinds.

105. This was flagged as a security violation, which led to the developers requesting SuperUser access for themselves.[113]

SEC Response: Disputed. The documents cited in paragraph 105 do not support Defendants' proposition that the developers requested SuperUser access as a result of a security violation having been "flagged." Rather, a reasonable juror could easily understand that the security violation was identified *because* of an access request submitted by the developers. The initial e-mail in the cited chain reads: "This request has brought to light three problems... They are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop...." [Def. Ex. 29 [SW-SEC00254254], at -4265]. The situation

[112] Def. Ex. 29 (SW-SEC00254254) at -265 (explaining that the developers were "using a shared login currently of a different SolarWinds employee," which "needs to stop"), -255 (explaining that the developers were using "shared logins with Superuser access to Production Backup data in order to pull data for billing" through two different APIs); Def. Ex. 2 (Rattray Rep.) ¶ 122.

[113] Def. Ex. 29 (SW-SEC00254254) at -257, -265-66; Def. Ex. 2 (Rattray Rep.) ¶ 122.

was later summarized in the same email chain, reflecting that while the development team "has a couple of shared logins with Superuser access to Production Backup data in order to pull data for billing (using 2 different API's)" they were unable to move forward with the "Backup O365 billing project because they need access to one more API to pull this data from Backup," [*id*. at -4255] and accordingly requested access to this additional API (*i.e.*, "application programming interface").

106. The request was evaluated and approved by Mr. Brown and other security personnel.[114]

SEC Response: Disputed. It is undisputed that Mr. Brown and other SolarWinds personnel evaluated the request, including Chris Day, who described the work of developers inside the production environment as "a significant security and Sox [sic] violation." [Def. Ex. 29 [SW-SEC00254254], at –4265]. It is also undisputed that Mr. Brown approved the request to provide the developers with SuperUser access, however the SEC disputes the statement in paragraph 106 that "other security personnel" approved the request as unsupported by any cited evidence. [*See* Def. Ex. 43 [SW-SEC00168780], at Columns K and M ("11/18/19: Risk reviewed by and accepted by Tim Brown;" "Approved By... Brown, Timothy")].

107. This event does not reflect that SolarWinds had a policy or practice of permitting employees to share accounts.[115]

SEC Response: Disputed. See response to paragraph 104.

---

[114] Def. Ex. 43 (SW-SEC00168780) at pdf p. 3 ("Risk reviewed and accepted by Tim Brown").

[115] Def. Ex. 50 (Graff Dep.) 172:16:21 ("Q. … So you can't infer from this e-mail that SolarWinds' systems were pervasively designed to give everyone read and write access; you're not drawing that conclusion, are you? A. No. There are other conclusions I'm drawing from it, but not that one."), 174:9-14 ("Q. [Y]ou're not contending that this shows that SolarWinds just pervasively granted everybody read/write access to all their systems; this was a single exception related to a particular team and a particular system? A. This particular incident, yes."); Def. Ex. 2 (Rattray Rep.) ¶¶ 123-25.

108. The fact that the developers' borrowing of someone else's account was flagged as a security violation when it was discovered reflects that SolarWinds had a policy of prohibiting employees from sharing accounts.[116]

SEC Response: Disputed. See response to paragraph 105. Further, as noted by Mr. Graff in his report, although the issue was brought to Mr. Brown's attention in November 2019, and he agreed it was a security violation that should be remediated by January 31, 2020, it "remained unaddressed until at least July 13, 2020—over five months beyond the date by which Mr. Brown agreed the risk must be remediated." [Def. Ex. 3 [Graff Rep.] ¶85 (citing Def. Ex. 43 [SW-SEC00168780])]. At best, this shows that SolarWinds thus disregarded any policy it might have had prohibiting employees from sharing accounts.

C. November 2019 Discovery and Remediation of "solarwinds123" Password

109. The SEC cites emails concerning a security researcher's report through which SolarWinds was alerted to and remediated a password—"solarwinds123"—on a third-party system, which did not meet the Company's password complexity requirements.[117]

SEC Response: Disputed. Undisputed that a security researcher reported to SolarWinds that he identified a "public Github repo[sitory] which is leaking ftp credential[s that] belongs to SolarWinds," and that the publicly available password of "solarwinds123" allowed "any hacker [to] upload malicious exe and update it with release SolarWinds product." [Def. Ex. 30 [SW-SEC00001464]. However, the reference to a "third-party system" is incomplete and therefore misleading. While the system from which the "solarwinds123" password was leaked was hosted by a third-party, Akamai, it provided access to SolarWinds files and consisted of a server from

[116] Def. Ex. 2 (Rattray Rep.) ¶¶ 123-25, 166-67.

[117] JS ¶¶187, 189; Def. Ex. 30 (SW-SEC00001464); Def. Ex. 31 (SW-SEC00001476) at -484.

which SolarWinds customers downloaded SolarWinds software, http://downloads.solarwinds.com. [*See* Zimmerman Decl. ¶4 ("SolarWinds software files would be distributed to customers by uploading the files to the Akamai Server, and then publishing links to the files on SolarWinds' customer websites... By clicking on the links, customers could download the files from the Akamai Server."); Brown Decl. Ex. H; SEC Ex. 34 [SW-SEC00407702-7707], at -7702 ("With that credential they could upload anything to downloads.solarwinds.com... The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present on our download site.")].

110. The password was for a single account on a single server hosted by Akamai, a third-party service provider (the "Akamai Server").[118]

SEC Response: Undisputed. It is also undisputed that, as reflected in the cited materials, a Senior Security Engineer at SolarWinds, Tomas Sejna, recognized that the publicly available password "allows attacker [sic] to upload files to our FTP download server," [Def. Ex. 31 [SW-SEC00001476], at -1484], *i.e.*, the Akamai Server, from which SolarWinds customers downloaded SolarWinds software [Zimmerman Decl. ¶4 ("SolarWinds software files would be distributed to customers by uploading the files to the Akamai Server, and then publishing links to the files on SolarWinds' customer websites... By clicking on the links, customers could download the files from the Akamai Server.")].

111. While SolarWinds' routine practice was to enforce password complexity requirements automatically on systems that provide for such functionality, the Akamai Server did

[118] Def. Ex. 31 (SW-SEC00001476) at -483; Def. Ex. 50 (Graff Dep.) 250:20-251:3; Def. Ex. 2 (Rattray Rep.) ¶¶ 175-77.

not provide functionality that would have allowed SolarWinds to enforce its password complexity requirements.[119]

SEC Response: Disputed to the extent it suggests that SolarWinds' Security Statement had such qualifying language. As discussed in Mr. Graff's rebuttal report in response to Dr. Rattray's opinions to this effect, the Security Statement "'covers *all* applicable information systems, applications, and databases,'" with no such exceptions. [*See* Def. Ex. 4 [Graff Reb. Rep.] ¶23 (quoting Def. Ex. 1 at 3 and adding emphasis)].

112. As a result, SolarWinds had to rely on manual compliance with the company's password complexity requirements with respect to the Akamai Server, which is always subject to the possibility of human error.[120]

SEC Response: Disputed. A reasonable juror could conclude that SolarWinds did not "ha[ve] to rely on manual compliance with the company's password complexity requirements with respect to the Akamai Server," because, as explained in the cited testimony of Mr. Graff when asked whether "you'd have to rely on human compliance with the password policy" on the Akamai server that "there are ways that you can automate the checking of password complexity" including "software available everywhere that checks for password complexity" such as "a script that run

[119] Def. Ex. 2 (Rattray Rep.) ¶ 175; Def. Ex. 52 (Johnson Dep.) 247:9-13 (discussing an analysis of "whether or not the product themselves can enforce password complexity control" where "[t]hose products are not part of the IT infrastructure for password management"); Zimmerman Decl. ¶ 6 ("[I]t is only possible to enforce password complexity automatically on systems that provide that functionality. SolarWinds did not have the ability to automatically enforce its password requirements on the Akamai Server," which "did not have any functionality that enabled SolarWinds to automatically enforce its password complexity requirements on user accounts."); Def. Ex. 50 (Graff Dep.) 250:15-19 ("Q. Okay. So you don't have any basis to contest that password complexity was enforced on active directory throughout the relevant period? A. For the systems under the control of active directory, I think that's right.").

[120] Def. Ex. 2 (Rattray Rep.) ¶ 175; Def. Ex. 50 (Graff Dep.) 255:21-256:7 ("Q. Okay. So for that part of the process, you'd require the person who was creating the password to manually make it complex; that's what you'd be depending on? A. In other words, if you want to enforce password complexity, you're saying you'd have to have the person that created the password follow that guideline? Q. Right. A. Yes, that sounds right. Q. And human compliance is always subject to error? A. I agree with that."); Zimmerman Decl. ¶ 6.

periodically and can check the password complexity of a given account." [Def. Ex. 50 [Graff Dep.] 251:16-252:14; *see also* Def. Ex. 4 [Graff Reb. Rep.] ¶23 (noting "the qualifying language that Dr. Rattray relied upon [in ¶175 of his report] was *missing* from the Security Statement")].

113. There is no evidence of any other non-complex passwords being used within SolarWinds during the Relevant Period or any evidence otherwise indicating that the use of non-complex passwords was a frequent problem at the Company.[121]

SEC Response: Disputed. A reasonable juror could credit the contemporaneous statements that that there were frequent problems with password management at the company, which would include a failure to meet password complexity requirements. Examples of these contemporaneous statements include instances in which "[p]assword requirements [were] not met" [SEC Ex. 8 [SW-SEC00001608-1634], at -1620]. Another example is a summary of control deficiencies from a SolarWinds SOX audit, similarly finding that "password history" configuration requirements were not met. [SEC Ex. 28 [SW-SEC00388330-8331], at PDF page 24 and 27]. As another example, SolarWinds' password for accessing VPN via X-Auth for limited device types failed to meet the company's password complexity requirements. According to a helpdesk email from February 2020, SolarWinds' X-Auth password at that time was "solarvpnpass," which does not comply with SolarWinds' password complexity requirements. [SEC Ex. 86 [HOLTZMAN_0011745], at PDF page *3].

[121] Def. Ex. 50 (Graff Dep.) 256:17-259:9 ("Q. But this is only one noncomplex password that you were able to find out of the thousands that would have been used at the company? Well, I wasn't looking for them. … Q. So you have no evidence that it was a frequent occurrence at SolarWinds to use noncomplex passwords? A. Frequent? I didn't really address frequency. But—see if I can agree with that. I don't think I have evidence that shows it was a frequent problem.").

114. While the security researcher who found the password was concerned that it could be used to distribute malicious software to alter the files SolarWinds made available to customers for download, in fact the password did not have this ability.[122]

SEC Response: Disputed. This paragraph is solely supported by two declarations: (i) Mr. Brown's declaration, which admits that he "did not personally know whether the compromised password could be used to corrupt any of our downloads" and defers to Mr. Zimmerman's knowledge of the issue [Brown Decl. ¶20], and (ii) Mr. Zimmerman's declaration, which does not stand for the proposition that the password did not have the ability detailed in paragraph 114, but rather that it was "highly unlikely." [Zimmerman Decl. ¶7] Moreover, Mr. Quitugua contradicted this statement in his SEC investigative testimony, confirming the security researcher's concern and saying that with the password at issue, "anybody could upload executables to the ... Akamai [server]." [SEC Ex. 36 [Quitugua Inv. Vol. II] 360:5-15]. In addition to that testimony, a reasonable juror could also credit contemporaneous statements by company personnel regarding the potential ability for attackers to use the "solarwinds123" password to distribute malicious software to the company's customers, including those detailed in Mr. Brown's declaration. [Brown Decl. ¶¶18-19 and Ex. H; SEC Ex. 34 [SW-SEC00407702-7707], at -7702 ("With that credential they could upload anything to downloads.solarwinds.com. I have assumed this was our main download site. . . . The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.")]. Additionally, as set forth in its Memorandum in Opposition to Summary Judgment filed today, the SEC objects to the Zimmerman Declaration on the grounds that Mr. Zimmerman was not listed as a witness in Defendants' Rule 26 disclosures or otherwise disclosed during discovery.

[122] Zimmerman Decl. ¶¶ 7-9; Brown Decl. ¶¶ 18-20.

115. There is no evidence that the password was ever discovered by a malicious actor.[123]

SEC Response: Undisputed. It is also undisputed that contemporaneous documents reflect that SolarWinds employees were not able to determine at the time whether "the compromised login information was not abused in the past," [Def. Ex. 31 [SW-SEC00001476], at -1480]. Further, while Mr. Zimmerman states that SolarWinds' subsequent "investigation found no indication that the Account was ever used by any unauthorized actor," [Zimmerman Decl. ¶10], as explained by Mr. Graff, "it can be difficult, once improper access has been granted to a repository, to *ever* ascertain whether files have been tampered with. Clever attackers have many tools at their disposal to cover their tracks, such as modifying the contents of a file in a malicious way while changing the file to conceal the tampering." [Def. Ex. 3 [Graff Rep.] ¶88]. Additionally, as set forth in its Memorandum in Opposition to Summary Judgment filed today, the SEC objects to the Zimmerman Declaration on the grounds that Mr. Zimmerman was not listed as a witness in Defendants' Rule 26 disclosures or otherwise disclosed during discovery.

116. The password was promptly changed after SolarWinds received the security researcher's report.[124]

SEC Response: Undisputed. It is also undisputed that by the time SolarWinds changed the password, it had been publicly available for approximately 20 months. [Zimmerman Decl. ¶5 (noting that the "solarwinds123" password was uploaded in March 2018 for a coding project "that, unknown to SolarWinds at the time, the intern accidentally made publicly searchable")]. Additionally, as set forth in its Memorandum in Opposition to Summary Judgment filed today, the

[123] Zimmerman Decl. ¶ 10.

[124] Zimmerman Decl. ¶ 10.

SEC objects to the Zimmerman Declaration on the grounds that Mr. Zimmerman was not listed as a witness in Defendants' Rule 26 disclosures or otherwise disclosed during discovery.

D. Control Deficiencies found in FY 2019 SOX Audit

117. The SEC cites a March 2020 spreadsheet prepared by Danielle Campbell, who ran SolarWinds' Internal Audit program, which indicated that a Fiscal Year 2019 SOX audit found certain "control deficiencies" relating to access controls and passwords.[125]

SEC Response: Undisputed.

118. None of the control deficiencies were deemed "significant deficiencies"—which must be reported to management—or "material weaknesses"—which must be reported to investors.[126]

SEC Response: Disputed only to the extent that "significant deficiencies" and "material weaknesses" must also be reported to the audit committee. [*See, e.g.,* "Auditing Standard 1305.04: Communications About Control Deficiencies in an Audit of Financial Statements" (stating "The auditor must communicate in writing to management and the audit committee all significant deficiencies and material weaknesses identified during the audit."), *available online at* https://pcaobus.org/oversight/standards/auditing-standards/details/AS1305) (last accessed June 12, 2025)].

[125] JS ¶188; Def. Ex. 36 (SW-SEC00388330) at -330; Campbell Decl. ¶¶ 3-5.

[126] Def. Ex. 36 (SW-SEC00388330) at pdf p. 6-7; Campbell Decl. ¶ 5; Def. Ex. 61 (Campbell Inv.) 180:10-16 (confirming that none of the control deficiencies were "significant" nor "material").

119. Rather, the deficiencies were all merely control deficiencies, which are minor by comparison and not considered to pose any risk to the accuracy of a company's financial statements (which is the focus of a SOX audit).[127]

SEC Response: Disputed only to the extent that the language is imprecise and therefore the meaning of "control deficiencies," as used in paragraph 119, is factually unclear. A control deficiency exists when "the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis." Both "significant deficiencies" and "material weaknesses" are types of control deficiencies. [*See, e.g.,* "Auditing Standard 2201: An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements," Appendix A – Definitions," *available online at* https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201) (last accessed June 12, 2025)]. The SEC also disputes defendants' characterization of the control deficiencies as "minor," as the cited declaration and testimony represent Ms. Campbell's subjective view and the characterization is otherwise unsupported by the evidence.

120. Ms. Campbell's spreadsheet specifically explained why none of the control deficiencies found was considered to have a "pervasive" impact.[128]

SEC Response: Undisputed. It is also undisputed that multiple entries pointed to other supposed controls that would "theoretically" lower the risk of those that were lacking; and that for

---

[127] Campbell Decl. ¶¶ 4-5, 9; Def. Ex. 61 (Campbell Inv.) 180:17-181:10 (explaining that a control deficiency is a "lower risk" compared to significant deficiencies and material weaknesses).

[128] Def. Ex. 36 (SW-SEC00388330) at pdf p. 6-7, column M; Campbell Decl. ¶ 6; Def. Ex. 61 (Campbell Inv.) 181:11-184:17 (explaining that all control deficiencies were reported to the Audit Committee "whether significant or not" and that Campbell was not aware of "any systemic issue with respect to the level of review and approvals required during the change management process").

two entries related to passwords, the spreadsheet's explanations included details about falling short of what "the control language requires." [*See, e.g.*, Def. Ex. 36 [SW-SEC00388330], at PDF page 6-7, Entry 9 ("control 2.2 (access provisioning) would theoretically act as a mitigating control as a way to ensure proper access changes are granted appropriately"); 27 ("Despite the deficiencies...there are mitigating controls that would theoretically work to address a missed quarterly review"); and 25 ("the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail just not to the extent that the control language requires.")].

121. Only two of the deficiencies related to password requirements.[129]

SEC Response: Disputed. While the summary on the first page of the cited attachment states that two deficiencies are related to password requirements, the accompanying dataset actually shows three – at Entry 7 (Backup User Access Management), 25 (RMM User Access Management), and 28 (Data Foundry Access). [Def. Ex. 36 [SW-SEC00388330], at PDF page 6-7].

122. Both deficiencies concerned systems on which password complexity requirements were enforced, but not password age and history requirements (*i.e.*, requirements that, after a certain number of days, passwords be changed to a password not previously used by the user).[130]

SEC Response: Disputed. The language in the document for Entries 7 and 25 says "complexity is enabled," not "enforced." For Entry 28, the document reads "Although password complexity was not set, other components of a secure password were configured, lowering the risk of inappropriate access to the servers." [Def. Ex. 36 [SW-SEC00388330], at PDF page 6-7].

---

[129] Campbell Decl. ¶ 7; Def. Ex. 36 (SW-SEC00388330) at pdf p. 6, lines 7 & 25.

[130] Campbell Decl. ¶ 7; Def. Ex. 36 (SW-SEC00388330) at pdf p. 6, lines 7 & 25.

123. The Security Statement says nothing about password age and history requirements.[131]

SEC Response: Undisputed. It is also undisputed that the Security Statement states that SolarWinds "enforce[s] the use of complex passwords," [Def. Ex. 1, at 3], which was not done as to Data Foundry Access as of March 2, 2020 [Def. Ex. 36 [SW-SEC00388330], at PDF page 7, Entry 28 ("password complexity was not set")]. Also, it is an issue for the jury whether "enforce the use of complex passwords" as used in the Security Statement [Def. Ex. 1, at 3] and "complexity is enabled" as used in Ms. Campbell's spreadsheet [Def. Ex. 36 [SW-SEC00388330], at PDF page 6, Entries 7, 25] have equivalent meanings, as defendants suggest.

124. Moreover, both password-related deficiencies were considered minor, because both of the systems at issue could generally only be accessed after logging into SolarWinds' corporate network, and password age and history requirements *were* enforced on the network login, through Active Directory.[132]

SEC Response: Disputed. With the exception of Ms. Campbell's post-deposition declaration, the evidence does not characterize the deficiencies as "minor," as defendants state in paragraph 124. In fact, the evidence shows that, into 2020, Quarterly Risk Reviews identified "significant deficiencies in user access management[,]" instances where "[p]assword requirements [were] not met," and "password history" requirements were not met, and acknowledged that "security processes [were] not consistently implemented." [SEC Ex. 7 [SEC-00001602-1607], at -1605; Def. Ex. 38 [SW-SEC00001602], at -1605; SEC Ex. 9 [SW-SEC00001582-1601], at -1587;

---

[131] Def. Ex. 1 (Security Statement) at 3.

[132] Def. Ex. 36 (SW-SEC00388330) (noting that both were considered "Low Risk" because "[i]nstances in which users are logging in outside of" the Active Directory were "not nearly as common"); Campbell Decl. ¶¶ 7-9.

SEC Ex. 28 [SW-SEC00388330-8331], at PDF page 8-9 (Entries 7 and 25) (identifying multiple company systems as not meeting password requirements because "maximum password age is not configured as required, nor is... a password history requirement.")].

IV. DOCUMENTS THE SEC RELIES ON AS TO THE SECURE DEVELOPMENT LIFECYCLE REPRESENTATION

A. January 2018 Email about "Feedback" on Secure Software Development

125. The SEC cites an email sent on January 30, 2018, approximately nine months before the Relevant Period, from Steven Colquitt, a Director of Engineering, to engineering managers, stating he had "gotten feedback that we don't do some of the things that are indicated" in the Security Statement's section on secure software development. Mr. Colquitt continued in the email:

> I want to make sure that you all have an answer to this. The simple response is: There is improvement needed to be able to meet the security expectation of a Secure Development Lifecycle. We will be working with teams throughout 2018 to begin incorporating the SDL into their development lifecycle. This begins with general SDL training for all Engineering along with several SDL pilots with specific teams in Q1. We'll continue to pragmatically roll out the SDL to additional teams each quarter."[133]

SEC Response: Undisputed. It is also undisputed that at the time of these statements the Security Statement, containing a representation that SolarWinds followed the Secure Development Lifecycle ("SDL"), was posted on SolarWinds' public website. [JS ¶25 (noting that SolarWinds first posted the Security Statement on November 16, 2017)].

[133] JS ¶190; Def. Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 2.

126. Around this time, Mr. Colquitt was working on a project to formalize and improve documentation of SolarWinds' secure development practices, as part of a company-wide project to prepare for new regulatory requirements coming into effect in May 2018.[134]

SEC Response: Disputed. Although the SEC agrees that SolarWinds was preparing for new regulatory requirements coming into effect in May 2018, the SEC disputes the characterization in paragraph 126 that Mr. Colquitt's work, if any, on the secure development lifecycle practices related to those new regulatory requirements, and/or the implication that any secure development practices were completed by May 2018. Multiple pieces of evidence show that SDL was still being adopted in 2019 and into 2020. *See, e.g.*:

- JS ¶193: A slide in the presentation titled "Goal for FY19: Grow Together: Joe's Goals, August's Goals, KPIs TBD" included the following goals: "[i]mprove security both in our products and our positioning," "[a]udit MSP Engineering training level and adoption of SDL (Secure Development Lifecycle)," and "[d]rive down the number of incidents introduced by MSP Engineering." [SEC Ex. 59 [SW-SEC-SDNY_00000004-0006], at PDF page *6];
- JS ¶194: A SolarWinds May 17, 2019, Security & Compliance Program Quarterly Review referred to the "Security Incident Improvement Plan"—a "[p]roject to operationalize and improve overall security for SolarWinds. This effort include[d] training (security and SDL)..." [SEC Ex. 21 [SW-SEC00001635-1651], at -1650];

[134] Colquitt Decl. ¶¶ 3-5; Def. Ex. 60 (Colquitt Dep.) 17:7-16 (noting Company's "preparing to be ready for GDPR compliance in May of 2018"), 58:19-25 ("The SDL was an overlay on top of that that exposed and gave visibility into these activities at a much higher level and centralized and formalized that documentation.").

- JS ¶195: A July 2019 document stated: "Design documentation overall is lacking and unstructured for the majority products. In addition, there is no governance in place to help provide consistency. These are crucial for threat modelling [sic] & other security activities in SSDLC. This should be covered by architecture, as part of the SSDLC process being formed." [SEC Ex. 45 [SW-SEC00166790-6799], at -6793;
- JS ¶197: A SolarWinds March 3, 2020, Quarterly Risk Review listed "[i]ncrease SDL adoption" as a "[k]ey [i]mprovement[]." [SEC Ex. 8 [SW-SEC00001608-1634], at -1611];
- JS ¶198: A May 22, 2020, Quarterly Risk Review also listed "[i]ncrease SDL adoption" as a goal of the "1H 2020 Improvement Plan." [SEC Ex. 48 [SW-SEC00148267-8294], at -8270];
- Turner Decl. Ex. 8: The Q4 2020 Quarterly Risk Review, dated October 27, 2020, stated under "Key Risks" that "[s]ecurity processes [were] not consistently implemented" and aspired to "[i]ncrease SDL awareness and adoption" for the "2H 2020 Improvement Plan." [SEC Ex. 9 [SW-SEC00001582-1601], at -1587].

127. Mr. Colquitt knew from years of working as a software engineer at SolarWinds that SolarWinds' development teams already conducted security testing as part of their software

development practices. He was seeking to overlay a new framework on these activities to make them more consistent across the organization and to improve documentation around them.[135]

SEC Response: Undisputed. But to the extent Defendants seek to use these activities to contest the plain language of Mr. Colquitt's January 30, 2018 email, this creates a dispute of material fact as the email itself indicates that Mr. Colquitt had received feedback that the company was not doing some of the things in the Security Statement with respect to the SDL.

128. As part of this effort, Mr. Colquitt developed new internal policy documentation describing the secure development processes that all teams should follow, which he labeled the Company's "Secure Development Lifecycle," or "SDL."[136]

SEC Response: Undisputed. But to the extent Defendants seek to use these activities to contest the plain language of Mr. Colquitt's January 30, 2018 email, this creates a disputed issue of material fact as the email itself indicates that Mr. Colquitt had received feedback that the company was not doing some of the things in the Security Statement with respect to the SDL.

129. Mr. Colquitt also developed new documentation requirements as part of the SDL, including a requirement that development teams prepare a Final Security Review before launching

---

[135] Colquitt Decl. ¶¶ 4, 13; Def. Ex. 60 (Colquitt Dep.) 58:19-25 ("The SDL was an overlay on top of that that exposed and gave visibility into those activities at a much higher level and centralized and formalized that documentation); 98:8-18 ("The SDL will help consolidate these activities, formalize and standardize these activities"); Def. Ex. 46 (Brown Dep.) 127:25-128:4 ("We … had at that period of time acquired a number of different solutions and a number of different companies, and those companies came in with their own practices. So standardizing knowledge across the organization was part of [the] goal [of Steven's project].").

[136] Colquitt Decl. ¶ 5; Def. Ex. 60 (Colquitt Dep.) 44:25-45:3 ("I was introducing a new process to overlay our security activities that we were labeling Secure Development Lifecycle, capital S, capital D, capital L. That was the title.").

a software release to document the security-related activities that went into the development of the release.[137]

SEC Response: Undisputed. But to the extent Defendants seek to use these activities to contest the plain language of Mr. Colquitt's January 30, 2018 email, this creates a disputed issue of material fact as the email itself indicates that Mr. Colquitt had received feedback that the company was not doing some of the things in the Security Statement with respect to the SDL.

130. Mr. Colquitt also developed an internal training for all software engineers at the company to familiarize them with the SDL framework. This training was designed for *all* engineers—not just those with a security-related role.[138] The purpose of the training was to increase visibility across the engineering organization into the Company's secure development practices and activities and to make sure everyone understood the importance of these activities.[139]

SEC Response: Undisputed. But to the extent Defendants seek to use these activities to contest the plain language of Mr. Colquitt's January 30, 2018 email, this creates a disputed issue of material fact as the email itself indicates that Mr. Colquitt had received feedback that the company was not doing some of the things in the Security Statement with respect to the SDL.

---

[137] Colquitt Decl. ¶ 5; Def. Ex. 60 (Colquitt Dep.) 31:25-32:6 (noting that goal of final security review was that "rather than having each team independently do their reviews and sign off, it was bringing them all together for a complete view of the posture, just to improve the visibility of what the teams have been doing from their testing and design").

[138] Colquitt Decl. ¶ 6; Def. Ex. 60 (Colquitt Dep.) 192:2-7 (noting that training included "[a]ll engineers, whether they were involved in security activities or not").

[139] Colquitt Decl. ¶ 6; Def. Ex. 60 (Colquitt Dep.) 195:9-19 ("Training broadly across the engineering teams introduced a formality and a consistency in our approach that some of those engineers might not have been familiar with prior, so this training brought that level of awareness to each of those individuals"); Ex. 46 (Brown Dep.) 127:11-128:8 (explaining that some engineers were uninvolved in security aspects of development and unaware of security requirements, "[s]o Steven's training was to level set across [the] organization" by "train[ing] every developer on development practices [to] make them aware of additional resources for secure development").

131. In late January, Mr. Colquitt was preparing to deliver this training. In anticipation of that, he thought it would be useful for all software development team members to be familiar with what SolarWinds publicly said about secure software development in the Company's Security Statement, which had only recently been added to the Company's website.[140]

SEC Response: Undisputed that Colquitt makes these statements in his 2025 declaration about what he was thinking when he wrote this email more than seven years ago, although the cited email itself does not provide such context.

132. On January 25, 2018, Mr. Colquitt sent the "Software Development Lifecycle" section of the Security Statement to all engineering managers, asking them to share it with their teams.[141]

SEC Response: Undisputed.

133. Five days later, on January 30, 2018, Mr. Colquitt got an email from one of these engineering managers, stating "[t]his is great progress in formalizing our security process," leading to a discussion in which Mr. Colquitt explained he would be beginning his general SDL trainings soon. Mr. Vrbecky wrote back:

> I think that would be great. It came back from teams as a feedback that we actually don't do things and actions that are in the statement. I'd say more accurate would be that teams are not fully aware about the scope of what we do and also what are we going to do by the end of Ql. For these kind of questions coming from team, I'd like managers to have canned answer.[142]

SEC Response: Undisputed.

---

[140] Colquitt Decl. ¶ 7; Def. Ex. 11 (SW-SEC00238141) at -141.

[141] Def. Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 7; Def. Ex. 60 (Colquitt Dep.) 94:11-95:7 (explaining that the inclusion of the SDL portion of the Security Statement was motivated by "awareness"), 198:9-12.

[142] Def. Ex. 12 (SW-SEC-SDNY_00055079) at -079; Colquitt Decl. ¶ 8.

134. Mr. Colquitt was not surprised that some engineers may not have known about the security testing that was already part of SolarWinds' software development processes.[143] He had asked engineering managers to share the excerpt from the Security Statement with *all* software engineers, not just those involved in the security aspects of development, so some of the recipients would not have been familiar with those aspects.[144] That is what Mr. Colquitt understood Mr. Vrbecky to mean by saying: "I'd say more accurate would be that teams are not fully aware about the scope of what we do."[145]

SEC Response: Disputed. At the outset, although Mr. Colquitt's deposition transcript was identified as Defendants' Exhibit 60, the transcript (apparently inadvertently) was not attached to Defendants' filing. For the convenience of the Court and parties, we have attached the transcript to our filing as SEC Exhibit 40 but continue to refer to the transcript as Defendants' Exhibit 60 in this filing. There is a material issue of fact given that in Mr. Colquitt's January 30, 2018, email to various SolarWinds engineering groups, he writes, "I've gotten feedback that we don't do some of the things that are indicated in the [Security Statement]. I want to make sure that you all have an answer to this." [SEC Ex. 41 [SW-SEC00238141-8142], at -8141]. Then, for the "simple response," Mr. Colquitt says, "There is improvement needed ***to be able to meet*** the security expectations of a Secure Development Lifecycle." [*Id.* (emphasis added)]. Mr. Colquitt's statement about not meeting the security expectations of the SDL is factually different from SolarWinds' position that SDL security expectations have been met, but engineering teams are just unaware of

[143] Colquitt Decl. ¶ 9; Def. Ex. 60 (Colquitt Dep.) 200:19-201:7 (acknowledging that "there were engineers on teams who probably weren't involved in aspects of things like pen testing, vulnerability testing, who didn't have direct knowledge that those activities were happening").

[144] Colquitt Decl. ¶ 9; Def. Ex. 60 (Colquitt Dep.) 198:9-23.

[145] Colquitt Decl. ¶ 9; Def. Ex. 60 (Colquitt Dep.) 200:19-201:7.

them. A reasonable juror could choose to credit the plain language of his email rather than his post-hoc explanation.

135. Mr. Colquitt responded to Mr. Vrbecky's email—which had asked for a "canned answer" that engineering managers could provide in response to any similar feedback—by sending another email to all engineering managers a few hours later, with a response they could provide, which is the email cited by the SEC.[146]

SEC Response: Undisputed.

136. In stating there was "improvement needed," Mr. Colquitt's intent was to encourage engineers to attend the trainings he was planning and to generate interest in the SDL framework that he had developed.[147]

SEC Response: Disputed. See the SEC's response to paragraph 134. In addition, the quoted language in paragraph 136 is incomplete and therefore misleading. The full sentence by Mr. Colquitt stated, "There is improvement needed to be able to meet the security expectations of a Secure Development Lifecycle." [SEC Ex. 41 [SW-SEC00238141-8142], at -8141]. Further, a reasonable juror could easily understand the plain language of the document to mean something different than what Mr. Colquitt claims for the first time in his post-deposition declaration. [*See* Def. Ex. 60 [SEC Ex. 40] [Colquitt Dep.] 208:4-17].

---

[146] Def. Ex. 11 (SW-SEC00238141) at -141; Colquitt Decl. ¶ 10; Def. Ex. 60 (Colquitt Dep.) 102:17-24.

[147] Colquitt Decl. ¶¶ 11-13; Def. Ex. 60 (Colquitt Dep.) 98:15-18, 101:4-19, 201:14-202:5 ("Q. And what type of improvements, again, was your SDL project focused on making? A. Again, mainly it brought awareness; two, it formalized the outputs, formalized documentation; and, third, it introduced some additional process that would facilitate bringing that documentation together").

137. Mr. Colquitt also believed there was improvement the Company needed to make to its software development practices—including around documentation, and raising security awareness across the engineering organization.[148]

SEC Response: Undisputed.

138. Mr. Colquitt did not mean to suggest that SolarWinds was not doing the types of security testing described in the Security Statement.[149]

SEC Response: Disputed. See the SEC's response to paragraph 134. In addition, a reasonable juror could easily understand the plain language of the document to mean something different than what Mr. Colquitt claims for the first time in his post-deposition declaration. [*See, e.g.*, Def. Ex. 60 [SEC Ex. 40] [Colquitt Dep.] 208:4-17 (Q: "[I]n your response to the managers when you're giving them an answer, you didn't say, [']We're doing all these things already,['] did you?" A: "That's not in my response." Q: "And you didn't...say to them that the teams are just not fully aware of the scope of what we're doing. Did you say that?" A: "I did not say that." Q: "You did say there is improvement needed to be able to meet the security expectations of a secure development lifecycle, right?" A: "Yes."); *see also* SEC Ex. 39 [SW-SEC00150761-0799], at -0761, -0762-0799 (2/1/2018 Colquitt email to Johnson and Pierce attaching presentation discussing needed training to implement the SDL)].

[148] Def. Ex. 60 (Colquitt Dep.) 98:15-18, 201:24-202:5; Colquitt Decl. ¶ 11.

[149] Def. Ex. 60 (Colquitt Dep.) 80:21-24 ("If you're asking me if we were applying the activities that supported what is listed in the security statement, the answer is yes"), 98:2-18; Colquitt Decl. ¶ 12.

B. February 2019 Slide about Goals for MSP Engineering

139. The SEC cites a slide from a deck sent in a February 13, 2019 email to all engineering staff within SolarWinds' MSP (Managed Service Provider) business line, which lists several goals for the group to "Grow Together."[150]

SEC Response: Undisputed.

140. The cited slide lists as among the "Goals" for FY 2019: "Improve security both in our products and our positioning," "Audit MSP Engineering training level and adoption of SDL (Secure Development Lifecycle)," and "Drive down the number of incidents introduced by MSP Engineering."[151]

SEC Response: Undisputed.

141. These statements simply reflected that SolarWinds wanted to continue improving its secure development practices and standardizing those practices across its product lines. In particular, the reference to "adoption of SDL" was a reference to Stephen Colquitt's project to standardize and formalize SolarWinds' already existing practices.[152]

SEC Response: Disputed. Paragraph 141 is conclusory and not supported by fact witnesses or documentary evidence. It also presents a material issue of fact given the document's statement, on its face, as to the "adoption of SDL," as compared with Defendants' position that SolarWinds was supplementing already existing practices. [SEC Ex. 59 [SW-SEC-SDNY_00000004-0006], at PDF page *6].

---

[150] JS ¶193; Def. Ex. 21 (SW-SEC-SDNY_00000004) at pdf p. 5; Def. Ex. 59 (Kim Dep.) 170:9-172:24.

[151] Def. Ex. 59 (Kim Dep.) 176:16-185:24; Def. Ex. 21 (SW-SEC-SDNY_00000004) at pdf p. 7.

[152] Def. Ex. 59 (Kim Dep.) 176:16-177:19 ("[O]ne of the things that I did want to make sure is that we continue improvement around the security stance and standardization across products. So here in terms of SDL, it's the project that I had Steven Colquitt and Tim Brown launch to see if we can better standardize and improve product security."); Def. Ex. 50 (Graff Dep.) 184:3-7 (agreeing "that cybersecurity is a process of continuous improvement.").

142. None of the stated goals were meant to suggest that MSP engineers pervasively failed to do security testing as part of their software development.[153]

SEC Response: Disputed. Paragraph 142 is conclusory and not supported by fact witnesses or documentary evidence. It also presents a material issue of fact given the document's statement, on its face, as to the "adoption of SDL," as compared with Defendants' position that the stated goals do not suggest that MSP engineers pervasively failed to do security testing. *See* [SEC Ex. 59 [SW-SEC-SDNY_00000004-0006], at PDF page *6].

C. Documents about Penetration Testing

1. Budget Item for External Penetration Testing in November 2018 Slide Deck

143. The SEC cites a November 2018 slide deck entitled "SolarWinds KBT Offsite DOIT and R&D," which included a slide titled, "FY18 Initiatives." A row of a chart on the slide contains an entry for "PEN Testing" with the note: "Unfunded in FY18. Plan to PEN test 8-10 products in 2019."[154]

SEC Response: Undisputed.

144. This was a reference to a specific budget item for *external* penetration testing—*i.e.*, penetration testing conducted by a third-party vendor, rather than penetration testing conducted internally by SolarWinds software engineers.[155]

---

[153] Def. Ex. 59 (Kim Dep.) 178:22-179:18 ("If I had to interpret it, he probably means the new SDL kind if initiative that Tim and Steven had launched [regarding documentation], and as part of their finding[] some additional training that they're putting in place to make sure that MSP engineering teams are, you know, getting trained on … the findings from that initiative."); Def. Ex. 59 (Kim Dep.) 117:9-118:11 (testifying that the "software development lifecycle" section of the Security Statement "was true at the time I was at SolarWinds" because "as stated here, things like vulnerability testing, regression testing, penetration testing and product security assessments were conducted on the products as part of the SDLC").

[154] JS ¶192; Def. Ex. 20 (SW-SEC00298924) at -934.

[155] Brown Decl. ¶¶ 13-14.

SEC Response: Undisputed.

145. External penetration testing required separate budget in order to engage the third-party vendor, unlike internal penetration testing that was conducted with personnel already on the SolarWinds payroll.[156]

SEC Response: Undisputed.

146. External penetration testing supplemented internal penetration testing done by SolarWinds.[157]

SEC Response: Undisputed.

147. The fact that a particular budget request for external penetration testing went unfunded for FY2018 does not imply that no internal penetration testing was done in FY2018.[158]

SEC Response: Undisputed.

148. The fact that a particular budget request for external penetration testing went unfunded for FY 2018 does not even imply that no external penetration testing was done in FY2018, as external penetration testing could have been funded through other means.[159]

SEC Response: Undisputed.

---

[156] Brown Decl. ¶ 14.

[157] Brown Decl. ¶ 14; Def. Ex. 46 (Brown Dep.) 134:10-22 ("[P]enetration testing was definitely done from an internal perspective and in some cases an external perspective"); Def. Ex. 23 SW-SEC00016539) at -5546 (excerpts from slide deck showing schedule for "External (3rd Party) Pen Testing Program" and "Internal Pen Testing Program").

[158] Brown Decl. ¶ 14; JS ¶148; Def. Ex. 60 (Colquitt Dep.) 48:1-23 ("We were doing … penetration testing"), 119:13-120:20 (testifying his teams did penetration testing); Def. Ex. 59 (Kim Dep.) 116:14-118:11 ("[P]enetration testing … w[as] conducted on the products as part of the SDLC."); 134:14-135:10; Def. Ex. 45 (Bliss Dep.) 134:9-135:2 (testifying "Software Development Life Cycle" part of the Security Statement "was accurate"); Colquitt Decl. ¶¶ 4, 12-13.

[159] Brown Decl. ¶ 1.

149. In fact, external penetration testing of certain products was completed in FY2018, including the Company's MSP and Cloud products.[160]

SEC Response: Undisputed.

2. July 2020 Slide about Testing in Final Security Reviews

150. The SEC cites a slide titled "ITOM Core Highlights and Asks" from a July 2020 deck prepared by Tim Brown, which states: "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release" and "[c]ustomers continue to actively engage 3rd party penetration testers as part of their compliance efforts[.]"[161]

SEC Response: Undisputed. It is also undisputed that the document contains additional language, including that "SolarWinds no longer under the radar" [SEC Ex. 50 [SW-SEC00006628-6648], at -6630]; that there were "compromised MSP admin accounts that do not have [multifactor authentication] turned on" [*id.* at -6632]; that "Low complexity, easily found vulnerabilities continue to trend in reports submitted to PSIRT from external researchers and customers" [*id.* at -6635]; and that "[s]ecurity reviews currently ad hoc – Add security reviews to the process" [*id.* at-6641].

151. The statement "Inconsistent internal security testing as part of product final security reviews don't always include web application testing before release" simply indicates that Final Security Reviews being prepared by software development teams did not "always" include web

[160] Brown Decl. ¶ 1; Def. Ex. 33 (SW-SEC00295588) (excerpts from slide deck titled "Summary of PEN Test results for MSP and Cloud performed Q2 2018" showing products covered by the testing; details of test results excluded).

[161] JS ¶200.

application testing results, which could mean either that the testing was not being done in those instances or that the results were not being included in the Final Security Reviews.[162]

SEC Response: Disputed. A reasonable juror could choose to credit the plain language of the document to mean that SolarWinds was not always doing this testing rather than credit the post-hoc explanations of the witnesses.

152. The statement does not indicate there was any pervasive failure to do web application testing.[163]

SEC Response: Disputed. The SEC disputes paragraph 152's "does not indicate there was any pervasive failure" description as conclusory and unsupported by the cited materials. A reasonable juror could choose to credit the failure to conduct web application testing, in conjunction with other failures noted about other documents, to determine there were pervasive problems with SolarWinds adherence to standard Secure Development Lifecycle protocols.

153. Under the statement there are references to "Checkmarx" and "Whitesource"—two testing products used by SolarWinds—indicating that these tools were available for engineers to use for web application testing.[164]

SEC Response: Undisputed.

154. Hundreds of records generated from the use of these tools during the Relevant Period were produced in discovery.[165]

SEC Response: Undisputed.

---

[162] Brown Decl. ¶¶ 15-16; Def. Ex. 45 (Bliss Dep.) 264:4-18 ("[M]y interpretation of this is this is an improvement on the overall program that you're looking at.").

[163] Brown Decl. ¶¶ 15-16.

[164] Def. Ex. 2 (Rattray Rep.) ¶ 95; Def. Ex. 45 (Bliss Dep.) 264:19-265:6 (CheckMarx and Whitesource are "tool[s] in the development life cycle.").

[165] Def. Ex. 2 (Rattray Rep.) ¶¶ 95-96 (referencing and citing these records).

155. The statement that "[c]ustomers continue to actively engage 3rd party penetration testers as part of their compliance efforts" simply indicates that some customers were conducting independent penetration testing of SolarWinds' products as part of their own compliance programs.[166]

SEC Response: Undisputed.

156. The statement does not imply that SolarWinds was not conducting penetration testing.[167]

SEC Response: Disputed. Right beneath that statement on the document is the statement that "Low complexity, easily found vulnerabilities continue to trend in reports submitted to PSIRT from external researchers and customers" [SEC Ex. 50 [SW-SEC00006628-6648], at -6635]. Taken together, a reasonable juror could conclude from the plain language of this contemporaneous document that SolarWinds was either frequently failing to conduct penetration testing, or that its penetration testing was of such poor quality that SolarWinds customers were the ones finding vulnerabilities that SolarWinds should have found. [*See also* Def. Ex. 3 [Graff Rep.] ¶188 and materials cited therein (customers often finding vulnerabilities that SolarWinds had missed should have alerted SolarWinds to its subpar practices); SEC Ex. 74 [SW-SEC00236723-6811], at -6759] (internal messages discussing *inter alia* that "the products are riddled[.] and obviously have been for many years[.] with nothing being found internally like this to this extent through testing[.]")].

---

[166] Brown Decl. ¶¶ 16-17; Def. Ex. 45 (Bliss Dep.) 265:19-266:5 ("My general experience with these customer inquiries is there are a number of penetration tools that were out there and we used some and they were good. Customers sometimes use a different tool and would not necessarily rely on what the company had done with their tool.").

[167] Brown Decl. ¶ 1; *see also* Def. Ex. 45 (Bliss Dep.) 134:9-135:2; 265:19-21 (Q: "Was this a statement that SolarWinds's penetration testing was inadequate? A: No."); Def. Ex. 60 (Colquitt Dep.) 48:1-23, 119:13-120:20; Ex. 59 (Kim Dep.) 116:14-118:11, 134:14-135:10.

D. Documents about Threat Modeling

1. May 2018 Email about Tool for Threat Modeling

157. The SEC cites a May 21, 2018 email from Rani Johnson to Tim Brown and Steven Colquitt and email with a subject line "Please confirm (particularly the threat modeling)." The body of the email included a list of tools used for "security capabilities," including PEN testing, vulnerability assessment/scanning, network monitoring, access control, and others.[168]

SEC Response: Undisputed.

158. Mr. Colquitt replied that, "I don't see a line item about threat modeling … but since you mentioned it. [Threat modeling] is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity. So I am not sure what you are looking for in terms of confirmation."[169]

SEC Response: Undisputed.

159. In saying "threat modeling" was "part of the SDL," Mr. Colquitt was saying it was part of the internal policy documentation he developed describing the secure development processes that all teams should follow.[170]

SEC Response: Disputed. Undisputed that Mr. Colquitt said the quoted language at his deposition. However, rather than credit Mr. Colquitt's explanations six years after writing the email, a reasonable juror could conclude that threat modeling is an inherent part of a Secure Development Lifecycle, based on the plain language of the document. Further, Microsoft's

---

[168] JS ¶191; Def. Ex. 17 (SW-SEC00237608) at -608-09; Def. Ex. 60 (Colquitt Dep.) 143:2-9.

[169] Def. Ex. 17 (SW-SEC00237608) at -608; Def. Ex. 60 (Colquitt Dep.) 138:17-20.

[170] Def. Ex. 60 (Colquitt Dep.) 139:1-12 (Q: "What did you mean that threat modeling is part of the SDL? A: … Currently the artifacts that were coming from the threat modeling that we were doing were not well documented …. And part of my project was to improve the artifacts that were coming from those activities in a more formal, formal manner.").

publicly available description of a Secure Development Lifecycle (a process Microsoft created) indicates that threat modeling is an inherent part of a Secure Development Lifecycle. [*See* https://www.microsoft.com/en-us/securityengineering/sdl/practices (last visited June 3, 2025) (outlining steps of the SDL, including "3. Perform security design review and threat modeling."); *see also* Def. Ex. 3 [Graff Rep.] ¶147 and materials cited therein (describing threat modeling as part of the SDL)].

160. The Security Statement itself does not mention anything about "threat modeling."[171]

SEC Response: Disputed. The SEC does not dispute that the words "threat modeling" do not appear in the Security Statement. But, for the reasons stated in response to paragraph 159, a reasonable juror could conclude that SolarWinds promise to adhere to the Secure Development Lifecycle contained an implicit promise to do threat modeling.

161. Mr. Colquitt understood the term "threat modeling" to be a broad term that can encompass many different types of activities designed to anticipate and address security risks in software functionality.[172]

SEC Response: Undisputed that Mr. Colquitt expressed this as his post-hoc personal belief.

---

[171] Def. Ex. 1 (Security Statement) at 3; Def. Ex. 60 (Colquitt Dep.) 139:3–24 ("[Threat modeling] was an additional thing that's not part of our security statement.").

[172] Def. Ex. 60 (Colquitt Dep.) 65:14-23 ("This exchange we just had where I explained that when I assess a particular requirement, I identify a risk and I mitigate that risk, that is threat modeling."), 144:23-145:8, 165:6-20 (stating that threat modeling is "an inherent aspect of implementing a mitigation to a security risk": "As an engineer when you are implementing a piece of functionality, you will assess the user or data interaction in that piece of functionality and you will assess whether there's a risk there. And if there is, you will put in a mitigation."), 206:5-207:2 ("[Threat modeling is] when you assess the risk that there might be an opportunity for someone to sort of get around the security that you've implemented in your product.").

162. In Mr. Colquitt's understanding, "[t]hreat modeling can be done verbally, it can be done on a piece of paper, it can be done on a whiteboard or you can use a formal tool to produce that documentation. There are multiple ways to do this exercise."[173]

SEC Response: Undisputed that Mr. Colquitt expressed this as his post-hoc personal belief.

163. In saying that "we are just barely beginning to understand how teams are going to be doing this activity," Mr. Colquitt was not "talking about doing the threat modeling itself," which "was already happening" at SolarWinds.[174]

SEC Response: Disputed. A reasonable juror could conclude from the face of the document that Mr. Colquitt was in fact talking about threat modeling when he wrote "[Threat modeling] is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity," [SEC Ex. 42 [SW-SEC00237608-7609], at -7608; JS ¶191], and could interpret contemporaneous documents, including a security evaluation performed by the company in 2019, as reflecting that threat modeling was still in the development stage at SolarWinds. For example, a July 2019 MSP Products Security Evaluation stated: "Design documentation overall is lacking and unstructured for the majority products. In addition, there is no governance in place to help provide consistency. These are crucial for threat modelling [sic] & other security activities in SSDLC. This should be covered by architecture, as part of the SSDLC process being formed." [SEC Ex. 45 [SW-SEC00166790-6799], at -6793]. Mr. Kim testified at his

[173] Def. Ex. 60 (Colquitt Dep.) 144:23-145:8; *see also* Def. Ex. 50 (Graff Dep.) 9:16-20 ("There are different levels of formalities you can use when you do cybersecurity assessments."); Def. Ex. 2 (Rattray Rep.) ¶¶ 207-208 ("'Threat modeling' is a loose term that can encompass virtually any effort to anticipate and address potential security threats as part of the software design process").

[174] Def. Ex. 60 (Colquitt Dep.) 142:16-19 ("Q: Okay. So you don't think you were talking about doing the threat modeling itself here? A: Threat modeling, no. It was already happening.").

deposition, with respect to the difference between the "secure development lifecycle" (*i.e.*, "SDL") and the "secure software development lifecycle" (*i.e.*, "SSDL" or "SSDLC"), that SDL "is secure development lifecycle, that is an internal name that Steve [Colquitt] and Tim [Brown] came up with. And sometimes it was called software security development lifecycle, SSDL...I'm sure you got documents that referred to it as SSDL as well." [SEC Ex. 43 [Kim Dep.] 140:1-141:20]. And Ms. Johnson testified at her deposition that secure software development lifecycle is "the way that employees who develop software utilize the practices of the SDL." [SEC Ex. 52 [Johnson Dep.] 160:25-161:4].

164. Mr. Colquitt was talking about how teams were going to be *documenting* the activity of threat modeling.[175]

SEC Response: Disputed. For the reasons set forth in the response to paragraph 163, a reasonable juror could choose not to credit this post-hoc explanation and instead interpret the plain language of the contemporaneous document to mean that Mr. Colquitt was talking about threat modeling itself, not merely documentation of it.

165. As part of his standardization project, Mr. Colquitt was still looking to "determine what options we had in terms of producing [] documentation" of threat modeling and "tracking that documentation."[176]

SEC Response: Disputed. For the reasons set forth in the response to paragraph 163, a reasonable juror could choose not to credit this post-hoc explanation and instead interpret the plain

[175] Def. Ex. 60 (Colquitt Dep.) 142:1-10 ("I wanted to improve the process. I was trying to determine what options we had in terms of producing that documentation and tracking that documentation that I had not yet settled on.").

[176] Def. Ex. 60 (Colquitt Dep.) 142:1-10.

language of the contemporaneous document to mean that Mr. Colquitt was talking about threat modeling itself, not merely documentation of it.

166. In particular, Mr. Colquitt was responding to an email sent from Ms. Johnson, who was collecting information about what sort of tooling was used for different security activities, and he was conveying that threat modeling was a "process" that would not necessarily be accomplished with a "formal tool."[177]

SEC Response: Disputed. Undisputed that Mr. Colquitt was responding to an email from Ms. Johnson and that her email listed several tools regarding security capabilities. Disputed that Mr. Colquitt was only referring to threat modeling not necessarily being accomplished with a formal tool. His email does not mention "formal tool" or "tool" but instead states that "[Threat modeling] is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity. So I am not sure what you are looking for in terms of confirmation." [SEC Ex. 42 [SW-SEC00237608-7609], at -7608; JS ¶191]. From this plain contemporaneous language, a reasonable juror could conclude that Mr. Colquitt was stating that SolarWinds was just barely beginning to understand how to perform threat modeling, rather than accepting the post-hoc interpretation now proffered for those words.

2. July 2019 MSP Products Evaluations

167. The SEC cites a document dated July 2019 titled, "MSP Products Evaluation."[178]

SEC Response: Undisputed.

168. The report covers three MSP products—RMM, NCentral and Backup.[179]

---

[177] Def. Ex. 60 (Colquitt Dep.) 144:10-145:8 (explaining that "I was implying that I wanted to improve the process," which would not necessarily involve a "formal tool").

[178] JS ¶195.

[179] JS ¶195.

SEC Response: Undisputed.

169. A line in the report states, "No threat modelling nor analysis is performed as part of any process (except MSP Backup Engineering)."[180]

SEC Response: Undisputed.

170. The SEC cites a similar evaluation for the MSP product MailAssure, dated December 2019, which contains a similar line.[181]

SEC Response: Undisputed. It is also undisputed that there is additional language in this document on which the SEC is relying, as set forth in Joint Statement of Undisputed Fact paragraph 195.

171. The SEC did not depose the authors of these documents in order to understand the meaning of this statement or what they meant exactly by "threat modeling."

SEC Response: Undisputed. It is also undisputed that the SEC questioned SolarWinds' designated representative, Jason Bliss, regarding this document during the Rule 30(b)(6) deposition of SolarWinds. [SEC Ex. 19 [Bliss Dep.] 270:17-271:7, 274:13-275:3].

172. SolarWinds' development teams within the MSP organization may not have done formalized threat modeling at the time these documents were prepared in July and December 2019, but they did analyze products for security risks and vulnerabilities.[182]

SEC Response: Disputed. The cited evidence does not support the asserted fact but instead consists of unfounded speculation by Mr. Colquitt during his deposition in which he literally

---

[180] JS ¶195.

[181] JS ¶196.

[182] Def. Ex. 60 (Colquitt Dep.) 170:22-171:5 ("I cannot speak to any of the MSP products or MSP engineering. I can speak to generally it's impossible to deliver security controls in a product without having done threat analysis."), 171:13-23 ("I don't understand what criteria they're using here to make that assessment. They may have been thinking of more of a formal process that they would like to achieve."), 206:15-207:2.

admits that "I cannot speak to any of the MSP products or MSP engineering" and "I do not understand what criteria they're using here to make that assessment." *See* [Def. Ex. 60 [SEC Ex. 40] [Colquitt Dep.] 170:10-171:23].

173. Final Security Reviews for releases of the RMM, NCentral and Backup products developed during the Relevant Period contain sections concerning "Vulnerabilities Addressed in Current Release," which in turn contain records of engineers identifying "risks" during the development process and proposing or implementing a "fix" or "mitigation" for each. These include records of such analysis being conducted around and before July 2019.[183]

SEC Response: Undisputed. It is also undisputed that Defendants' cited evidence to support this assertion, the report of Defendants' expert, Dr. Rattray, notes that the documents and testimony he reviewed "contradict[] the remark that '[n]o threat modelling [sic] nor analysis is performed as part of any process.'" [Def. Ex. 2 [Rattray Rep.] ¶213]. Given the lack of substantive analysis by Dr. Rattray it is unclear and therefore disputed as to what, if any, threat modeling or analysis was actually performed in the documents he cites. This is especially the case given that the documents on which Dr. Rattray purported to rely included a largely blank document [SEC Ex. 60 [Rattray Dep.] 235:21-240:21] and other documents where he simply looked at the headers on the documents and "didn't look at the documents for the reasons that that was unnecessary." [*Id.* at 240:25-243:2. *See also id.* at 244:24-245:10; SEC Ex. 61 [SW-SEC-SDNY_00069825-9828] (cited at Rattray Dep. 237:16); [SEC Ex. 62 [SW-SEC-SDNY_00055006] (same at Rattray Dep. 241:11)].

[183] Def. Ex. 2 (Rattray Rep.) ¶¶ 212-13.

E. June 2020 Email about Orion Improvement Program

174. The SEC cites an email exchange from June 2020 with the subject line "SDL and Orion Improvement Program," in which a SolarWinds engineer stated in part "Do we have SDL process enforced for Orion Improvement Program server? If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected." Another engineer responded, "I don't believe we cover OIP today with the SDL, but we should." The SEC has argued that the fact that the Company's "SDL"—*i.e.*, its secure development process—did not cover the Orion Improvement Program (OIP) at the time contradicts the Security Statement.[184]

SEC Response: Undisputed.

175. The Security Statement's section on software development discusses what SolarWinds does "to increase the resiliency and trustworthiness of *our products*."[185]

SEC Response: Undisputed that the quoted language appears in the Security Statement. It is also undisputed that the emphasis supplied in the quoted statement does not appear in the Security Statement.

176. OIP was not a SolarWinds product or a component of a SolarWinds product.[186]

---

[184] JS ¶199; AC ¶¶ 131–35.

[185] Def. Ex. 1 (Security Statement) at 3; Def. Ex. 50 (Graff Dep.) 286:7-15 (Q: "Would you agree that the term 'products' typically refers to the things that a company sells to its customers? A: Yes."); Def. Ex. 2 (Rattray Rep.) ¶¶ 197-98 ("SolarWinds' software development lifecycle [in] the Security Statement refers to 'our products'—a term that [Mr. Graff] himself uses in his report to refer to software sold to SolarWinds' customers.").

[186] Def. Ex. 48 (Brown Inv. Vol. II) 380:12-381:4("[T]he OIP server that's talked about is our internally-hosted server … . That's what OIP is. … [I]t's something inside of our environment. It's not a product we sell, it's not a solution that is, you know, offered to customers or anything like that."), 394:20-395:12; Def. Ex. 50 (Graff Dep.) 288:22-25 (Q: "[W]ould you agree that the OIP software application was not a product that SolarWinds sold to customers? A: Yes, that's my understanding."); 290:7-12 ("Well, the OIP application was not a product, I agree with that."); Def. Ex. 2 (Rattray Rep.) ¶ 199 ("OIP was not software that SolarWinds *customers* used; it resided on SolarWinds own network and was used *by SolarWinds*.").

SEC Response: Disputed. It is undisputed that OIP was not a SolarWinds product. It is disputed whether it was part of or a component of a SolarWinds product. OIP was hosted inside SolarWinds' network. But it communicated with SolarWinds customers and took information from them about their usage of the Orion suite of products in order to improve that product. [Def. Ex. 2 [Rattray Rep.] ¶¶199-200 (citing and quoting materials including Brown Dep.); Def. Ex. 48 [Brown Inv. Vol. II] 395:4-7 ("[OIP] was built internally for the specific purpose of collecting information and helping customers with their deployment."); *see also* Def. Ex. 3 [Graff Rep.] ¶¶170-175]. Thus, whether OIP is fairly considered part of a SolarWinds product is a question of fact for a jury to determine. This is especially the case as SolarWinds own employees recognized that OIP should be part of the SDL at the time. [*See* SEC Ex. 49 [SW-SEC00000673-0678], at -0678].

177. OIP was an internal business application that SolarWinds used to collect Orion usage information from customers who agreed to provide it, in order to help advise customers on how to improve their deployment of the software.[187]

SEC Response: Disputed. Because OIP communicated with and routinely collected Orion usage information from customers, it cannot fairly be considered solely an "internal" business application. *See* response to paragraph 176 above. Otherwise, undisputed.

[187] Def. Ex. 48 (Brown Inv. Vol. II) 394:20-395:7 ("So these are called Bizapps, business applications. One of those business applications is OIP. That business application was built internally for the specific purpose of collecting information and helping customers with their deployment."); Def. Ex. 53 (Johnson Inv. Vol. II) 207:13-16 ("Q. And what is your understanding of what the Orion Improvement Program is? A. It was a server that collected information related to customers' usage of Orion.").

178. The OIP application ran on SolarWinds' own server, not on customer infrastructure.[188]

SEC Response: Undisputed. It is also undisputed that OIP routinely communicated with and received information from customers' servers regarding their Orion usage. *See* Response to Paragraph 176 above.

179. The suggestion in the cited email chain to "cover OIP … with the SDL" was made in the context of SolarWinds' investigation of an incident reported by the Department of Justice's U.S. Trustee Program ("USTP")—the same incident that is discussed in the SEC's Amended Complaint involving "U.S. Government Agency A."[189]

SEC Response: Undisputed.

180. In initially responding to the report, SolarWinds' InfoSec team was concerned that an attacker might be trying to *attack SolarWinds* through the OIP server.[190]

SEC Response: Disputed. SolarWinds engineers were explicit in stating that the OIP should be covered by the SDL because the "OIP API [application programming interface] is not authenticated so it can accept content for any user," that the API was "exposed externally so everybody can access it," and that a compromise of OIP's server could have "***disastrous***" effects,

---

[188] Def. Ex. 48 (Brown Inv. Vol. II) 380:12-381:4 ("The OIP server sits inside of our environment and it takes information from clients to essentially improve their product. But it's a separate application, not something that's commercial. It's something that's inside of our environment to talk to."); Def. Ex. 49 (Cline Dep.) 15:6-13 (explaining that BizApps are SolarWinds "business applications" and "very much focused on the application side that the business runs off of"); Def. Ex. 2 (Rattray Rep.) ¶¶ 199-200.

[189] AC ¶¶ 268-278; Def. Ex. 2 (Rattray Rep.) ¶ 202.

[190] Def. Ex. 48 (Brown Inv. Vol. II) 381:18-382:9 ("So our theory with this is that … either the box [i.e., server] that [USTP] installed [Orion] on was a dirty box and had [malicious code on it], or that, you know, the box itself had been compromised without us and that that [malicious code] was attacking SolarWinds with that OIP layer. So that's why you'll see a lot of hardening on OIP. … We essentially brought in everybody to look at this traffic and this incident."); Def. Ex. 2 (Rattray Rep.) ¶ 202.

possibly including "***taking over all customer installations***." [SEC Ex. 49 [SW-SEC00000673-0678], at -0678 (emphasis added)].

181. In that context, the Infosec team sought to harden the OIP server against attack by applying the same sort of testing to OIP that the Company would do as part of its software development lifecycle for customer products. The decision to do so was not made because OIP was such a product or because the testing was supposed to have been done earlier, but because this particular incident raised a concern that OIP was potentially being targeted as part of an attack on SolarWinds.[191]

SEC Response: Disputed. This conclusory statement regarding the intentions and thoughts of the SolarWinds employees at the time is but one possible interpretation from the undisputed facts recited above. Another possible interpretation is that SolarWinds employees realized that as functional part of the Orion suite of products that communicated with customers servers, OIP was something that already should have been covered by the SDL. A reasonable juror does not have to accept Defendants' preferred explanation from these possibilities.

[191] Def. Ex. 48 (Brown Inv. Vol. II) 388:10-21 ("[W]hen you build a product for internal use, not a product but a service that you're going to use internally[,] that doesn't necessarily follow the same processes that when we build the products from the outside. But we implemented a number of those processes around the OIP server and investigated the server itself and then, you know, made some changes to the OIP server to make sure that—you know, that it was hardened against attacks. Although we couldn't tell what the attack was from the data we had, [we] essentially looked everywhere we could and put as many safeguards in place on the OIP server so it wouldn't affect us."); Def. Ex. 2 (Rattray Rep.) ¶¶ 202-04.

Dated: June 13, 2025

Respectfully submitted,

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann
(SDNY Bar No. CB-7317)
Christopher J. Carney
John J. Todor (admitted *pro hac vice*)
Kristen M. Warden (admitted *pro hac vice*)
William B. Ney (admitted *pro hac vice*)
Benjamin Brutlag
(SDNY Bar No. BB-1196)
Lory Stone (admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5986 (Bruckmann)
202-551-2379 (Carney)
202-551-4661 (Warden)
202-551-5381 (Todor)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
WardenK@sec.gov
BruckmannC@sec.gov
CarneyC@sec.gov
TodorJ@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission

CERTIFICATE OF SERVICE

I hereby certify that on June 13, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

/s/ Christopher M. Bruckmann
Christopher M. Bruckmann